TR-4931: VMware Cloud on Amazon Web Services とゲストコネクトによる災害復旧

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

目次

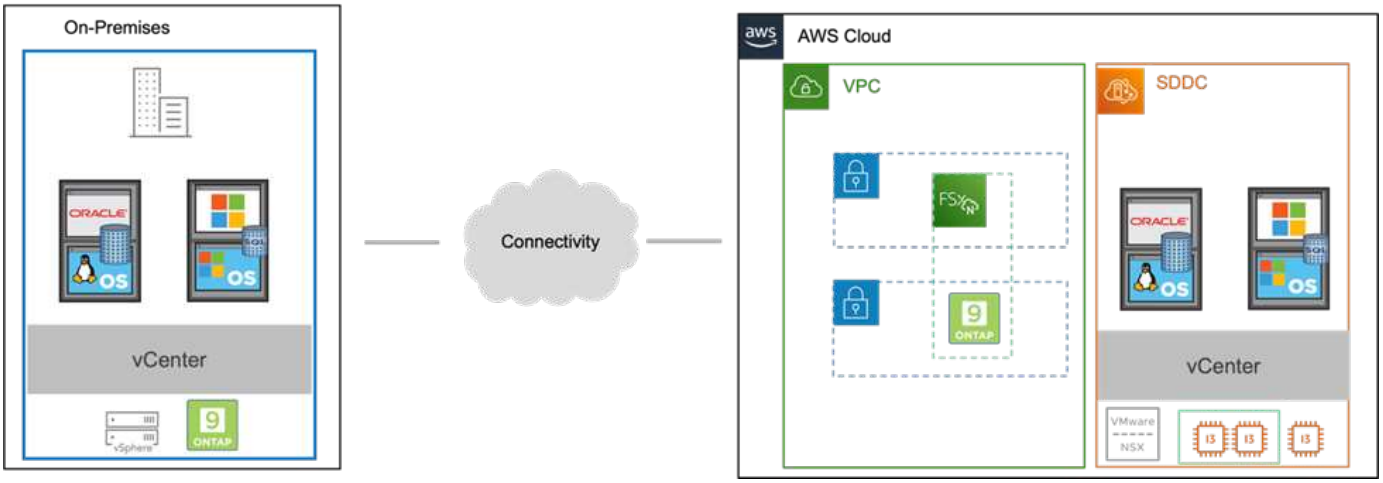
TR-4931: VMware Cloud on Amazon Web Services とゲストコネクトによる災害復旧

大規模な障害が発生した場合にビジネスクリティカルなアプリケーションを迅速に復旧できるようにするために、組織にとって実証済みの災害復旧 (DR) 環境と計画が不可欠です。このソリューションは、オンプレミスと VMware Cloud on AWS の両方で、VMware およびNetAppテクノロジーに重点を置いた DR ユースケースのデモンストレーションに重点を置いています。

概要

NetApp はVMware との統合において長い歴史を誇ります。これは、仮想化環境のストレージ パートナーとしてNetAppを選択した何万もの顧客によって証明されています。この統合は、クラウド内のゲスト接続オプションや、最近の NFS データストアとの統合でも継続されます。このソリューションは、一般的にゲスト接続ストレージと呼ばれるユースケースに重点を置いています。

ゲスト接続ストレージでは、ゲスト VMDK は VMware によってプロビジョニングされたデータストアに展開され、アプリケーション データは iSCSI または NFS に格納され、VM に直接マップされます。次の図に示すように、Oracle および MS SQL アプリケーションを使用して DR シナリオを説明します。



前提、前提条件、コンポーネントの概要

このソリューションを展開する前に、コンポーネントの概要、ソリューションを展開するために必要な前提条件、およびこのソリューションを文書化する際に行われた仮定を確認してください。

"DRソリューションの要件、前提条件、および計画"

SnapCenterでDRを実行する

このソリューションでは、 SnapCenter はSQL Server および Oracle アプリケーション データに対してアプリケーション整合性のあるスナップショットを提供します。この構成は、 SnapMirrorテクノロジーと組み合わせることで、オンプレミスのAFFと FSx ONTAPクラスター間の高速データ レプリケーションを実現します。さらに、Veeam Backup & Replication は仮想マシンのバックアップと復元機能を提供します。

このセクションでは、バックアップとリストアの両方におけるSnapCenter、 SnapMirror、および Veeam の構成について説明します。

次のセクションでは、セカンダリ サイトでフェイルオーバーを完了するために必要な構成と手順について説明します。

SnapMirror関係と保持スケジュールを構成する

SnapCenter は、長期アーカイブと保持を目的として、プライマリ ストレージ システム内 (プライマリ > ミラー) およびセカンダリ ストレージ システム (プライマリ > ボールト) のSnapMirror関係を更新できます。そのためには、 SnapMirrorを使用して、宛先ボリュームとソース ボリューム間のデータ複製関係を確立し、初期化する必要があります。

ソースと宛先のONTAPシステムは、Amazon VPC ピアリング、トランジットゲートウェイ、AWS Direct Connect、または AWS VPN を使用してピアリングされたネットワーク内にある必要があります。

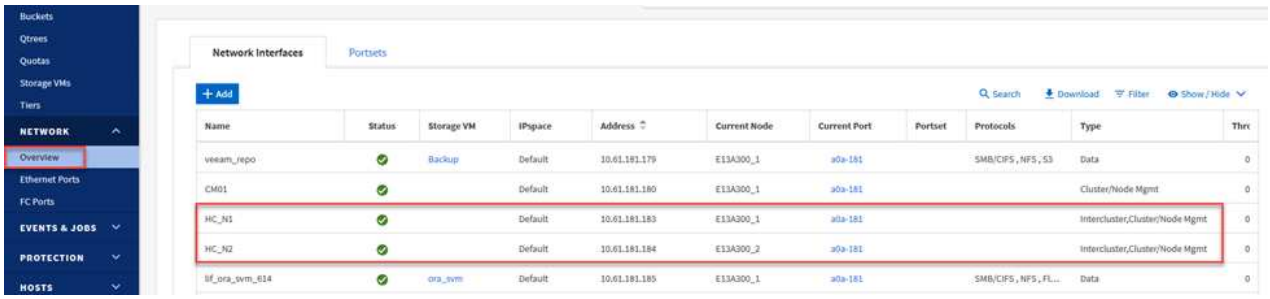
オンプレミスのONTAPシステムと FSx ONTAPの間にSnapMirror関係を設定するには、次の手順が必要です。

参照 "FSx ONTAP – ONTAPユーザーガイド"FSx とのSnapMirror関係の作成の詳細については、こちらをご覧ください。

送信元と宛先のクラスタ間論理インターフェースを記録する

オンプレミスにあるソースONTAPシステムの場合、System Manager または CLI からクラスタ間 LIF 情報を取得できます。

1. ONTAP System Manager で、[ネットワークの概要] ページに移動し、FSx がインストールされている AWS VPC と通信するように設定されているタイプ: クラスタ間の IP アドレスを取得します。



2. FSx のクラスター間 IP アドレスを取得するには、CLI にログインして次のコマンドを実行します。

```
FSx-Dest::> network interface show -role intercluster
```

```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
FsxId0ae40e08acc0dea67
            inter_1      up/up    172.30.15.42/25    FsxId0ae40e08acc0dea67-01
                                                                   e0e     true
            inter_2      up/up    172.30.14.28/26    FsxId0ae40e08acc0dea67-02
                                                                   e0e     true
2 entries were displayed.
```

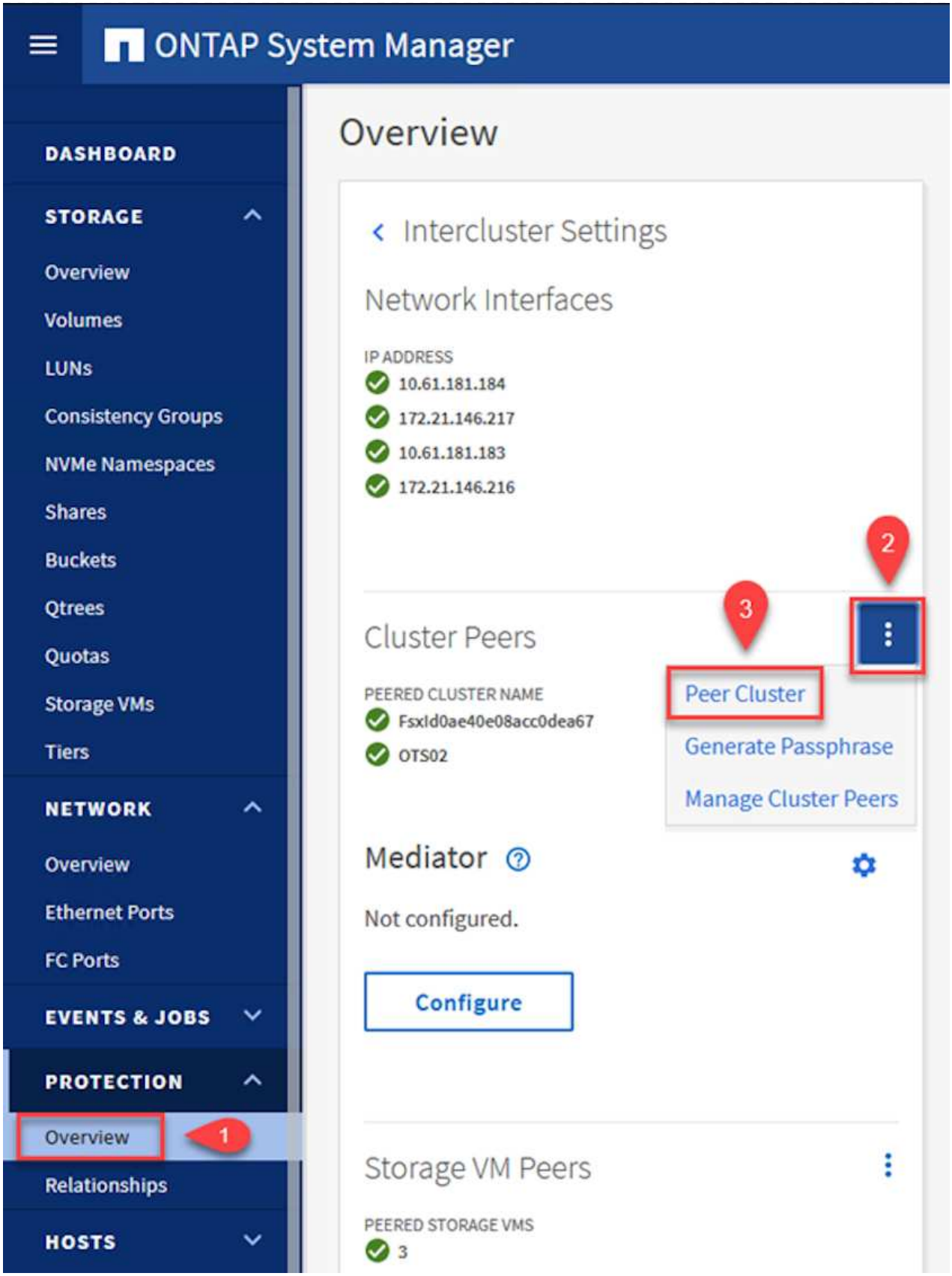
ONTAPと**FSx**間のクラスタピアリングを確立する

ONTAPクラスタ間のクラスタ ピアリングを確立するには、開始側のONTAPクラスタで入力した一意のパスフレーズを、他のピア クラスタで確認する必要があります。

1. 宛先FSxクラスタでピアリングを設定するには、 `cluster peer create`指示。プロンプトが表示されたら、後でソース クラスターで作成プロセスを完了するために使用する一意のパスフレーズを入力します。

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. ソース クラスタでは、 ONTAP System Manager または CLI を使用してクラスタ ピア関係を確立できます。 ONTAP System Manager から、[Protection] > [Overview] に移動し、[Peer Cluster] を選択します。

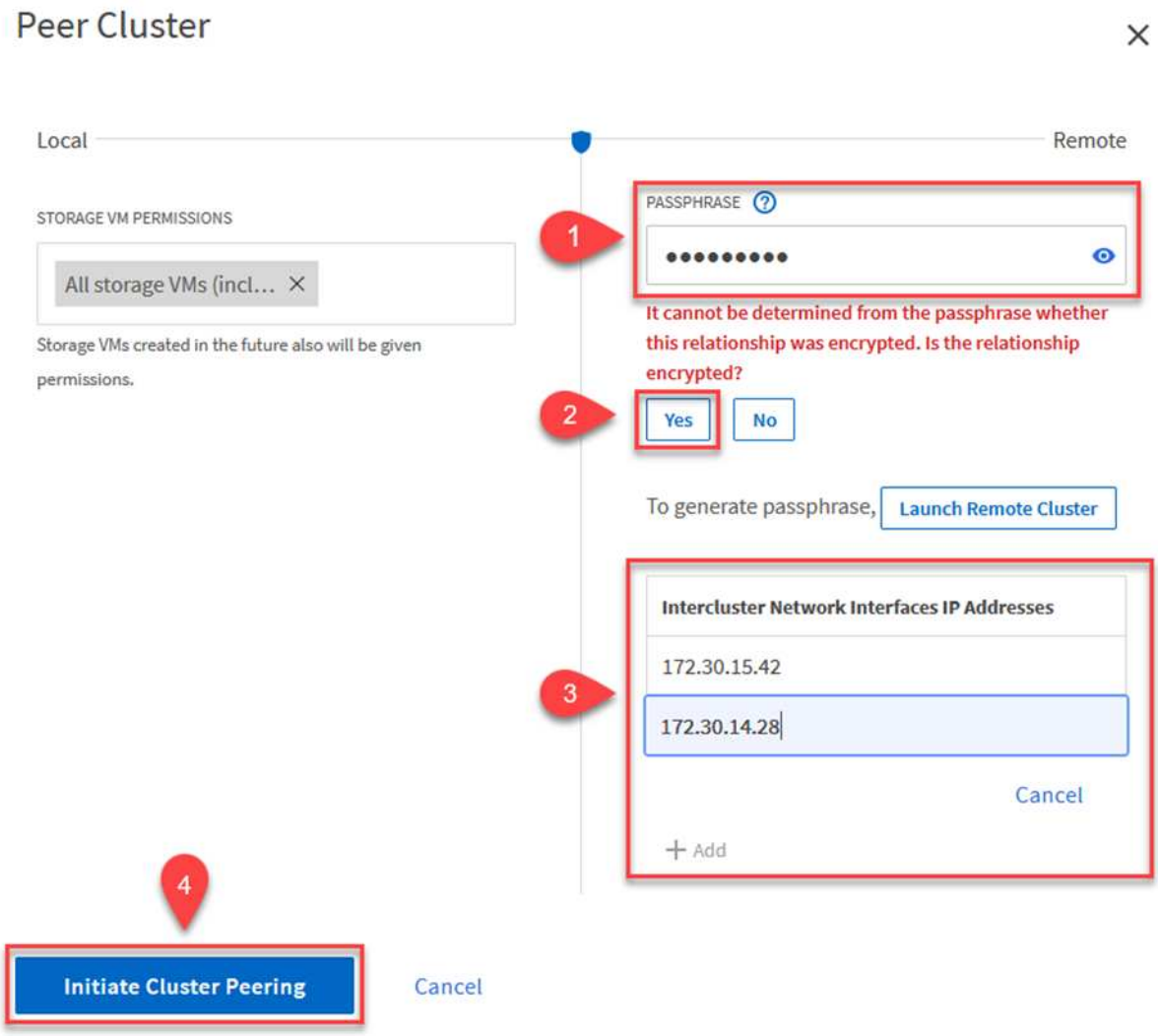


3. [ピア クラスター] ダイアログ ボックスで、必要な情報を入力します。
   a. 宛先 FSx クラスターでピア クラスター関係を確立するために使用されたパスフレーズを入力します。

b. 選択 `Yes`暗号化された関係を確立します。

c. 宛先 FSx クラスタのクラスタ間 LIF IP アドレスを入力します。

d. プロセスを終了するには、「クラスター ピアリングの開始」をクリックします。



4. 次のコマンドを使用して、FSx クラスターからクラスター ピア関係のステータスを確認します。

```
FSx-Dest::> cluster peer show
```

```
FsxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability   Authentication
------------------------- --------------------- -------------- --------------
E13A300                   1-80-000011           Available      ok
```

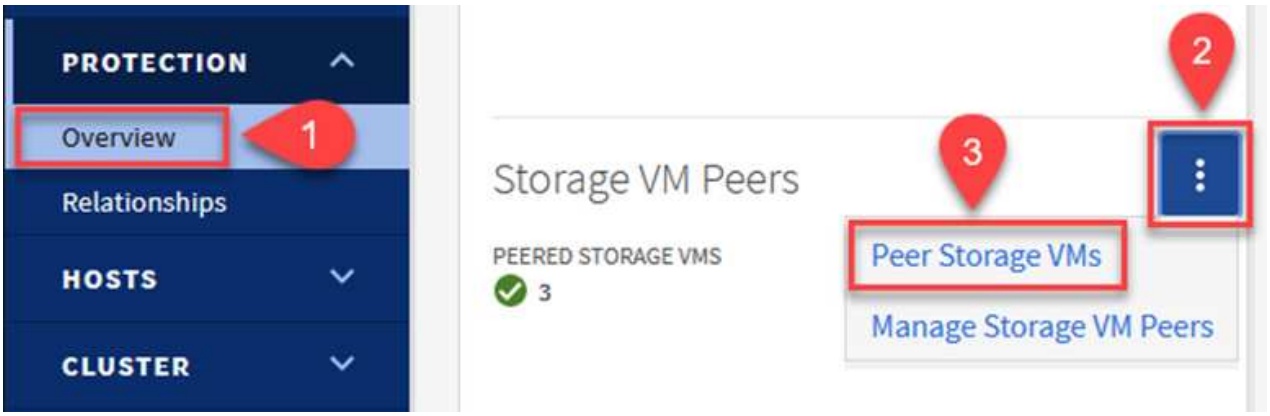
SVMピアリング関係を確立する

次の手順では、 SnapMirror関係になるボリュームを含む宛先ストレージ仮想マシンとソース ストレージ仮想マシン間の SVM 関係を設定します。

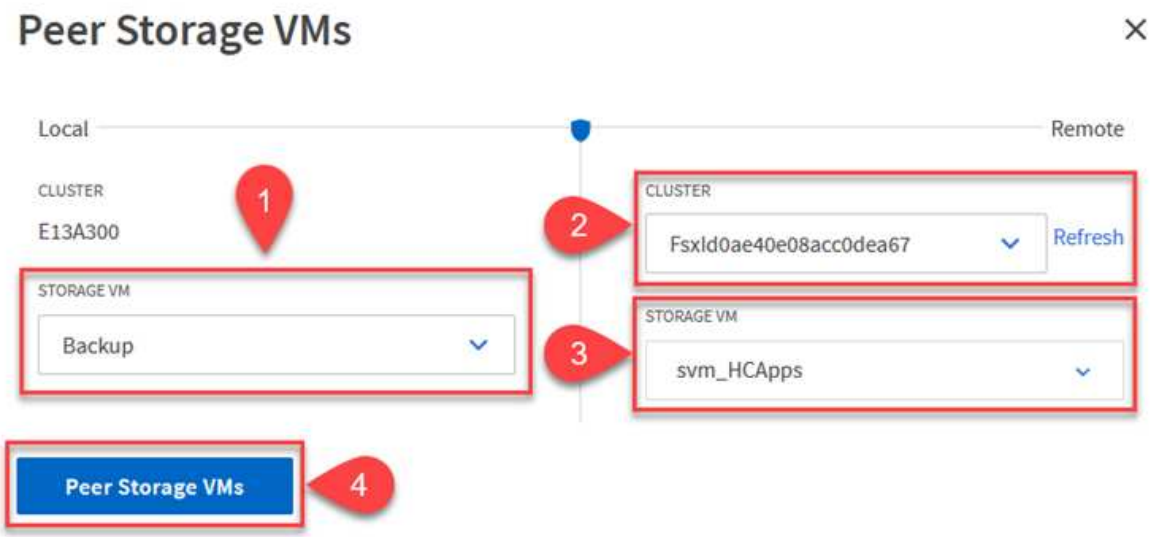
1. ソース FSx クラスターから、CLI から次のコマンドを使用して SVM ピア関係を作成します。

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. ソースONTAPクラスタから、 ONTAP System Manager または CLI のいずれかを使用してピアリング関係を受け入れます。
3. ONTAP System Manager から、[Protection] > [Overview] に移動し、[Storage VM Peers] の下の [Peer Storage VMs] を選択します。



4. ピア ストレージ VM のダイアログ ボックスで、必須フィールドに入力します。
   - ソースストレージVM
   - 宛先クラスター
   - 宛先ストレージVM



5. SVM ピアリング プロセスを完了するには、[ピア ストレージ VM] をクリックします。

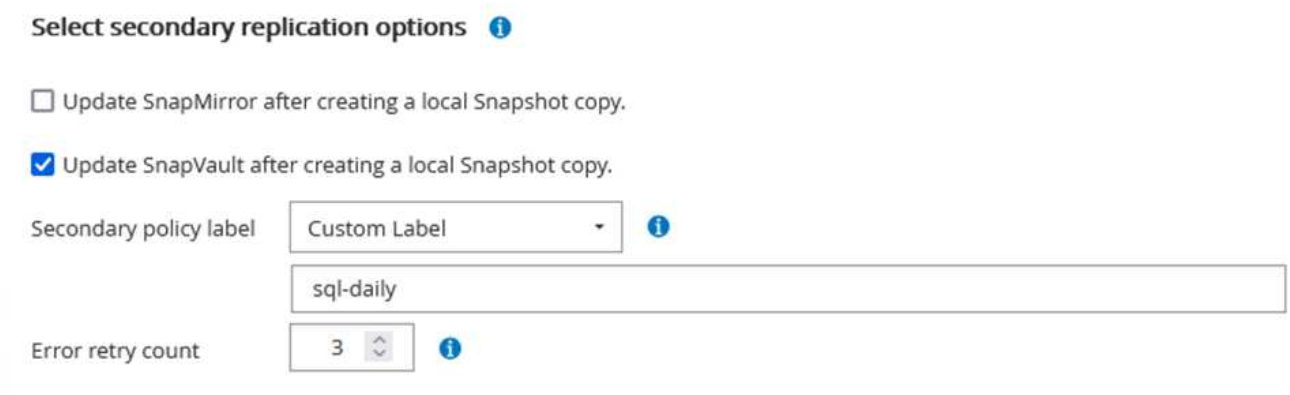
スナップショット保持ポリシーを作成する

SnapCenter は、プライマリ ストレージ システム上にスナップショット コピーとして存在するバックアップの保持スケジュールを管理します。これは、 SnapCenterでポリシーを作成するときに確立されます。 SnapCenter は、セカンダリ ストレージ システムに保持されるバックアップの保持ポリシーを管理しません。これらのポリシーは、セカンダリ FSx クラスター上に作成され、ソース ボリュームとSnapMirror関係にある宛先ボリュームに関連付けられたSnapMirrorポリシーを通じて個別に管理されます。

SnapCenterポリシーを作成するときに、 SnapCenterバックアップの作成時に生成される各スナップショットのSnapMirrorラベルに追加されるセカンダリ ポリシー ラベルを指定するオプションがあります。

セカンダリ ストレージでは、これらのラベルは、スナップショットの保持を強制する目的で、宛先ボリュームに関連付けられたポリシー ルールと照合されます。

次の例は、SQL Server データベースとログ ボリュームの毎日のバックアップに使用されるポリシーの一部として生成されたすべてのスナップショットに存在するSnapMirrorラベルを示しています。



SQL Serverデータベース用のSnapCenterポリシーの作成の詳細については、 "SnapCenterのドキュメント" 。

まず、保持するスナップショット コピーの数を指定するルールを含むSnapMirrorポリシーを作成する必要があります。

1. FSx クラスターにSnapMirrorポリシーを作成します。

```
FSx-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. SnapCenterポリシーで指定されたセカンダリ ポリシー ラベルと一致するSnapMirrorラベルを使用して、ポリシーにルールを追加します。

```
FSx-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

次のスクリプトは、ポリシーに追加できるルールの例を示しています。

```
FSx-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy
Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

各SnapMirrorラベルと保持するスナップショットの数 (保持期間) に対して追加のルールを作成します。

宛先ボリュームを作成する

ソース ボリュームからのスナップショット コピーの受信者となる FSx 上の宛先ボリュームを作成するには、FSx ONTAPで次のコマンドを実行します。

```
FSx-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

ソースボリュームと宛先ボリューム間の**SnapMirror**関係を作成する

ソース ボリュームと宛先ボリュームの間にSnapMirror関係を作成するには、FSx ONTAPで次のコマンドを実行します。

```
FSx-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

SnapMirror関係を初期化する

SnapMirror関係を初期化します。このプロセスは、ソース ボリュームから生成された新しいスナップショットを開始し、それを宛先ボリュームにコピーします。

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

オンプレミスで **Windows SnapCenter**サーバーを展開および構成します。

Windows SnapCenter Server をオンプレミスに導入

このソリューションは、 NetApp SnapCenterを使用して、SQL Server および Oracle データベースのアプリケーション整合性のあるバックアップを取得します。仮想マシン VMDK をバックアップする Veeam Backup & Replication と組み合わせることで、オンプレミスおよびクラウドベースのデータセンター向けの包括的な災害復旧ソリューションが提供されます。

SnapCenter softwareはNetAppサポート サイトから入手でき、ドメインまたはワークグループ内に存在する Microsoft Windows システムにインストールできます。詳細な計画ガイドとインストール手順については、 "NetAppドキュメント センター" 。

SnapCenter softwareは以下から入手できます。 "このリンク" 。

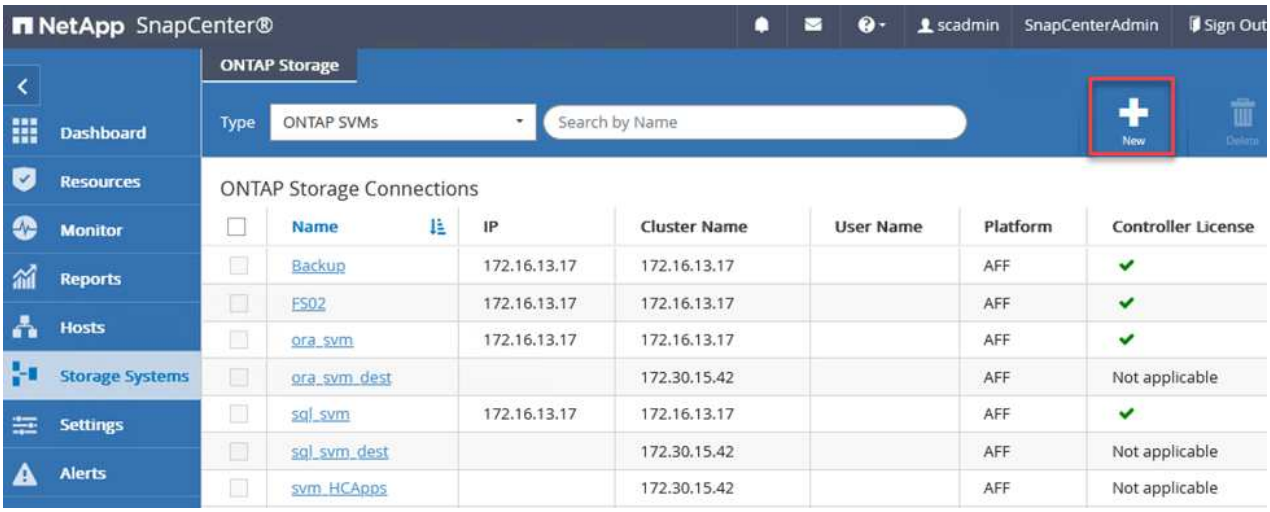
インストール後、*https://Virtual_Cluster_IP_or_FQDN:8146* を使用して Web ブラウザーからSnapCenter コンソールにアクセスできるようになります。

コンソールにログインしたら、SQL Server および Oracle データベースのバックアップ用にSnapCenter を構成する必要があります。

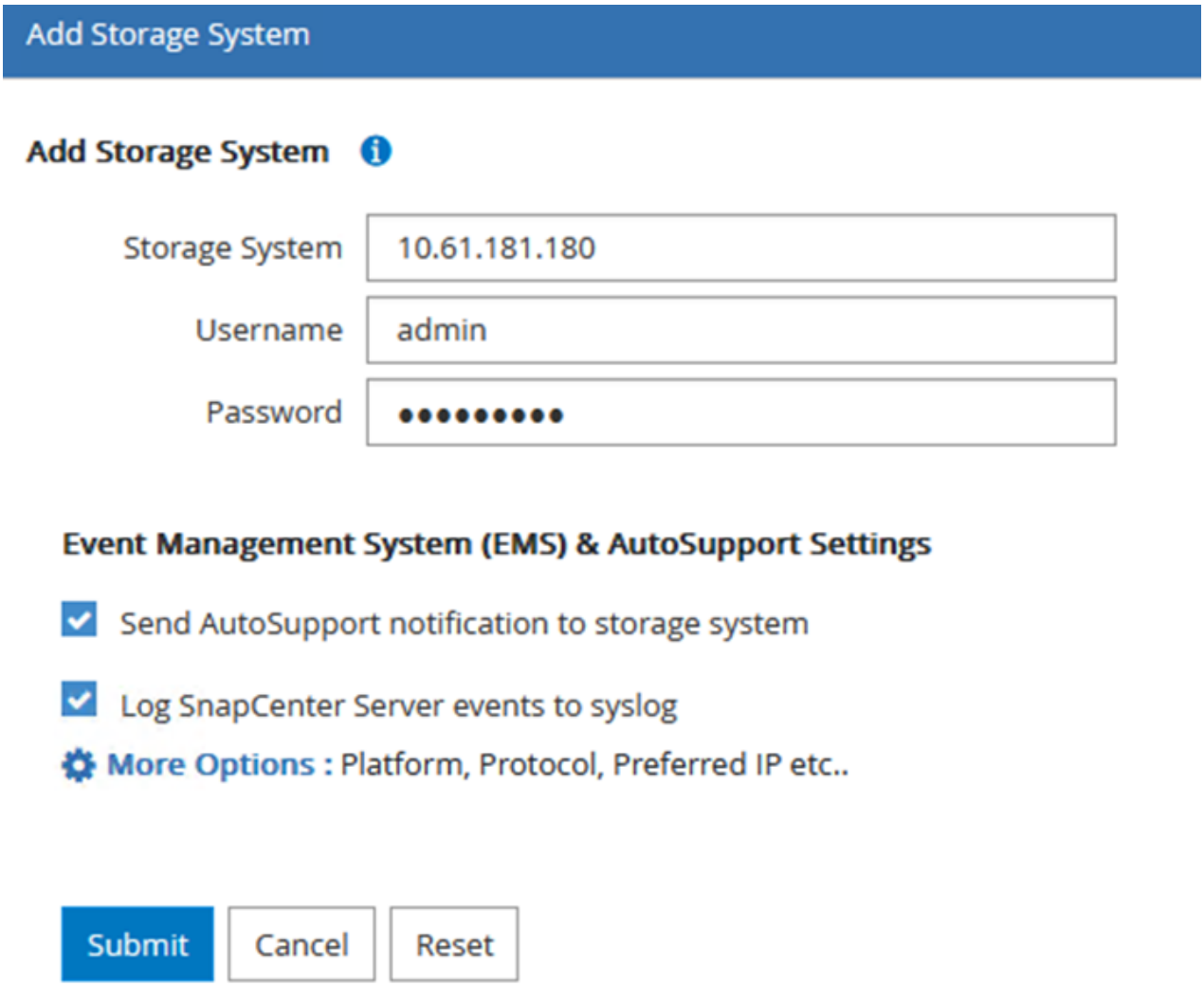
SnapCenterにストレージコントローラを追加する

SnapCenterにストレージ コントローラーを追加するには、次の手順を実行します。

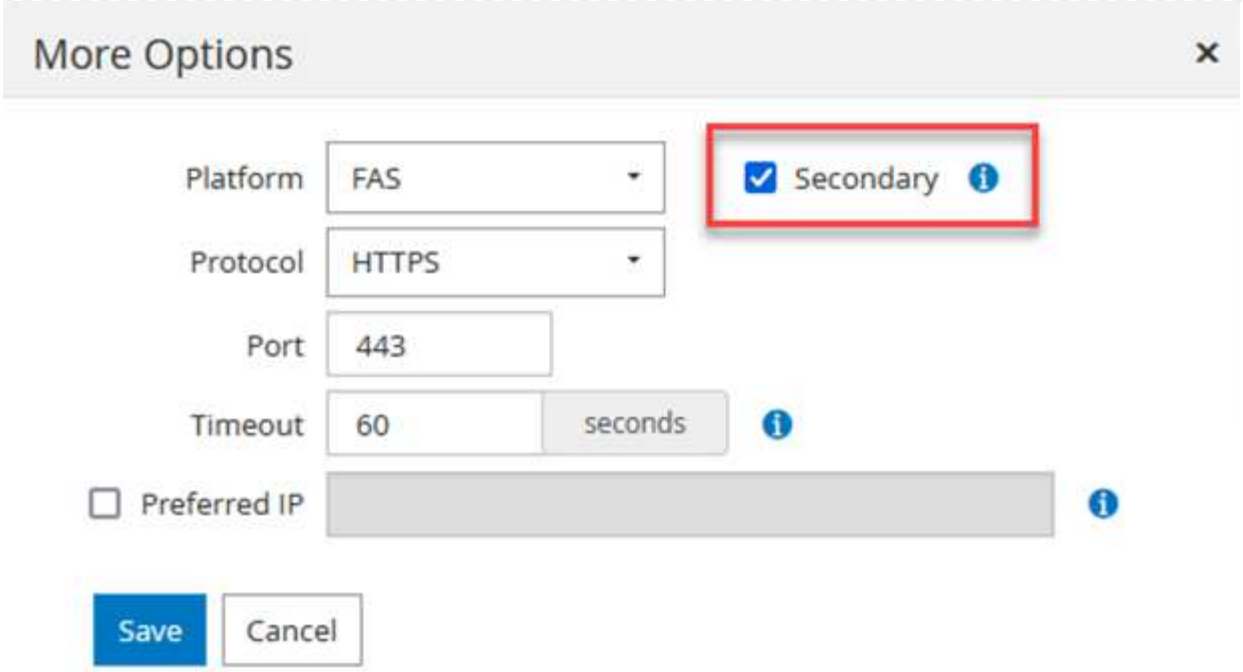
1. 左側のメニューから [ストレージ システム] を選択し、[新規] をクリックして、ストレージ コントローラーをSnapCenterに追加するプロセスを開始します。



2. [ストレージ システムの追加] ダイアログ ボックスで、ローカルのオンプレミスONTAPクラスターの管理 IP アドレスとユーザー名およびパスワードを追加します。次に、「送信」をクリックしてストレージ システムの検出を開始します。



3. このプロセスを繰り返して、FSx ONTAPシステムをSnapCenterに追加します。この場合、「ストレージ システムの追加」ウィンドウの下部にある「その他のオプション」を選択し、「セカンダリ」のチェック ボックスをクリックして、FSx システムをSnapMirrorコピーまたはプライマリ バックアップ スナップショットで更新されたセカンダリ ストレージ システムとして指定します。

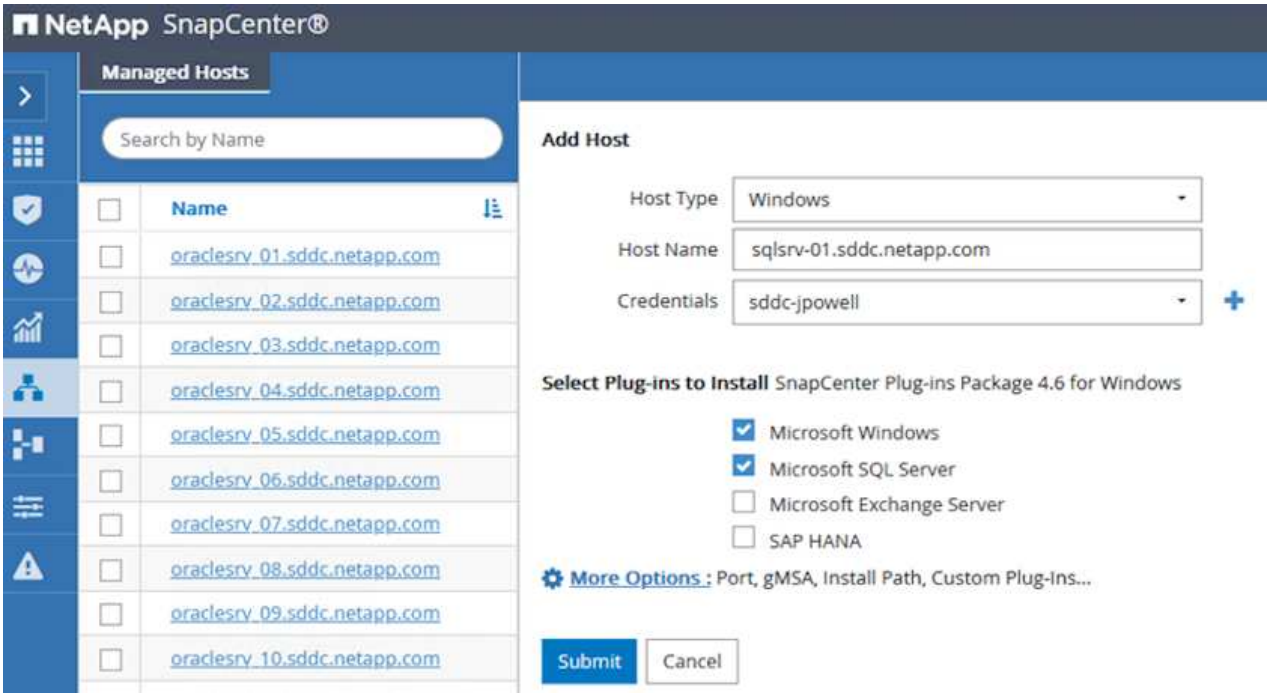


SnapCenterへのストレージシステムの追加に関する詳細については、次のドキュメントを参照してください。 "このリンク" 。

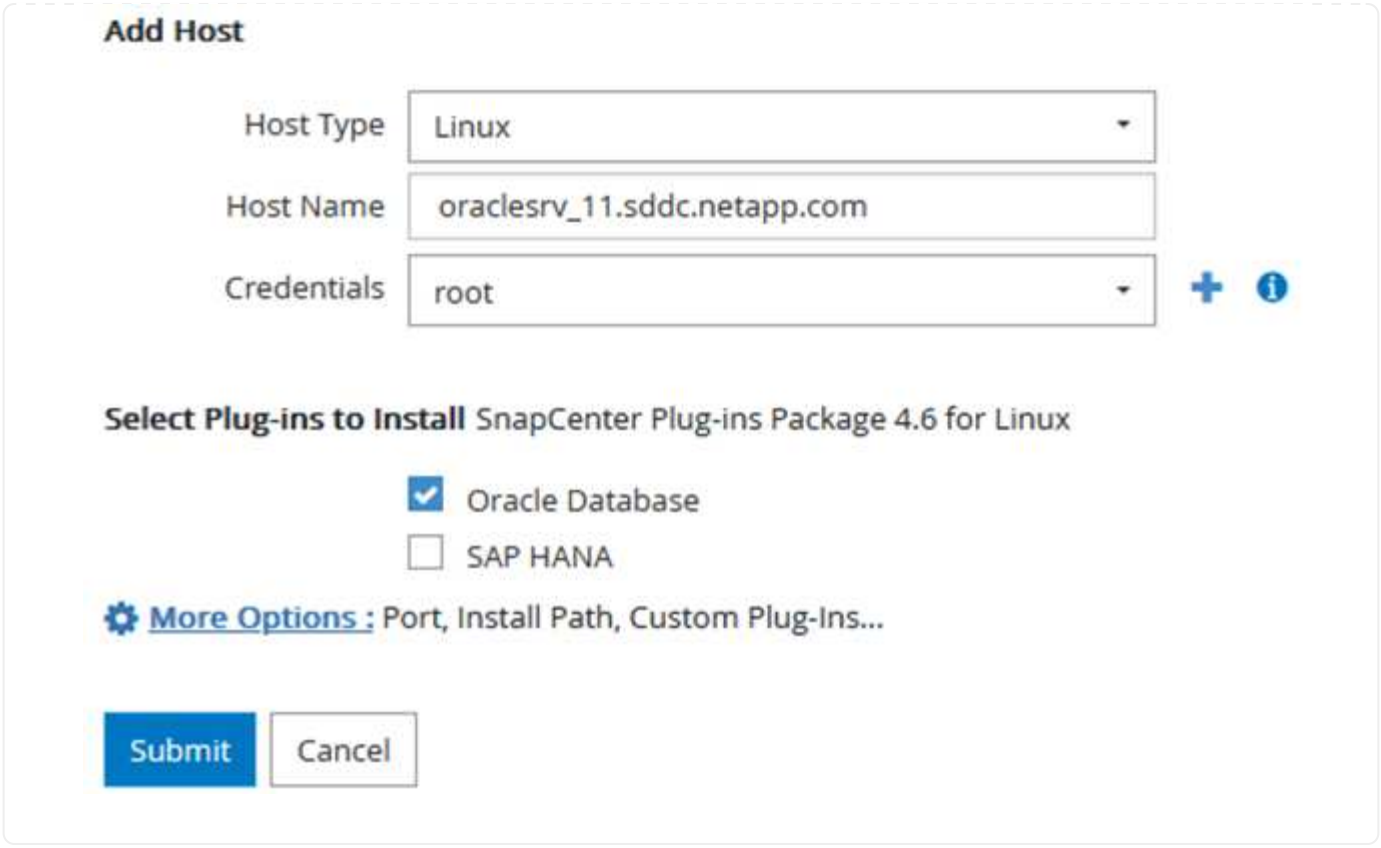
SnapCenterにホストを追加する

次のステップは、ホスト アプリケーション サーバーをSnapCenterに追加することです。プロセスは SQL Server と Oracle の両方で同様です。

1. 左側のメニューから [ホスト] を選択し、[追加] をクリックして、 SnapCenterにストレージ コントローラーを追加するプロセスを開始します。
2. [ホストの追加] ウィンドウで、ホスト タイプ、ホスト名、およびホスト システムの資格情報を追加します。プラグインの種類を選択します。 SQL Server の場合は、Microsoft Windows および Microsoft SQL Server プラグインを選択します。



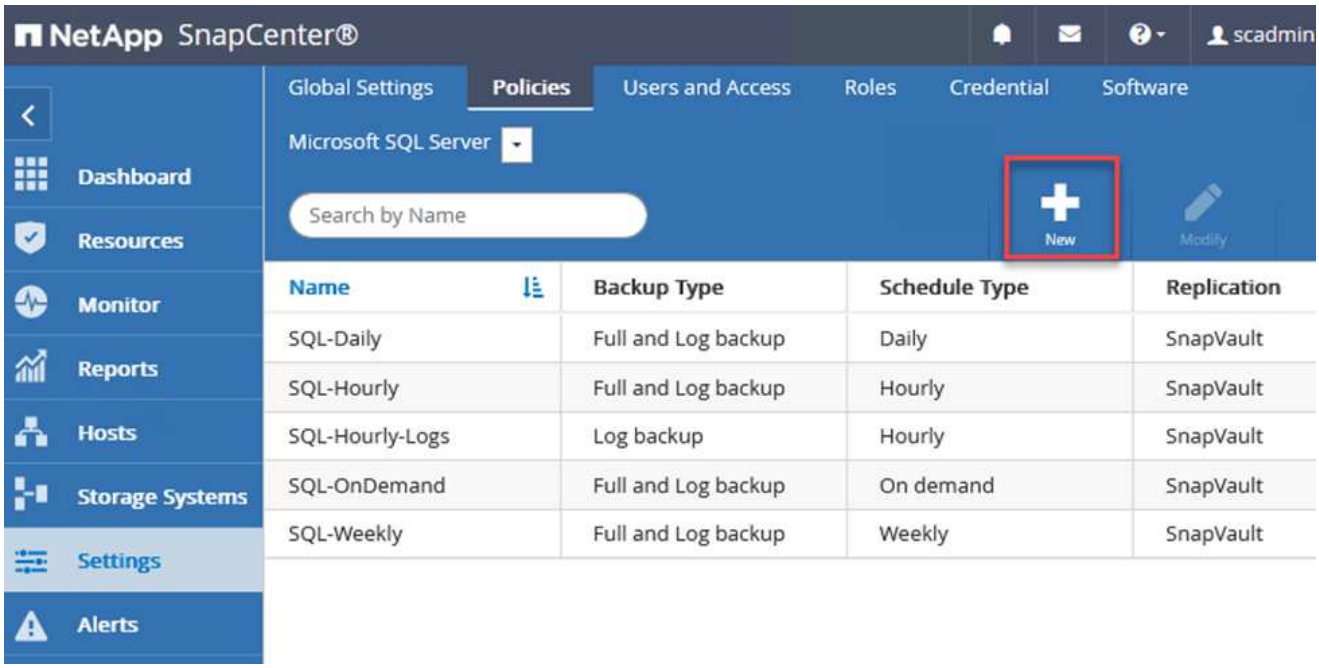
3. Oracleの場合、「ホストの追加」ダイアログボックスの必須フィールドに入力し、Oracle Database プラグインのチェックボックスをオンにします。「送信」をクリックすると検出プロセスが開始され、ホストがSnapCenterに追加されます。


Add Host
Host Type
Linux
Host Name
oraclesrv_11.sddc.netapp.com
Credentials
root
Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Linux
Oracle Database
SAP HANA
More Options : Port, Install Path, Custom Plug-Ins...
Submit
Cancel

SnapCenterポリシーを作成する

ポリシーは、バックアップ ジョブに従う特定のルールを確立します。これらには、バックアップ スケジュール、レプリケーション タイプ、 SnapCenter がトランザクション ログのバックアップと切り捨てを処理する方法などが含まれますが、これらに限定されません。

SnapCenter Web クライアントの [設定] セクションでポリシーにアクセスできます。



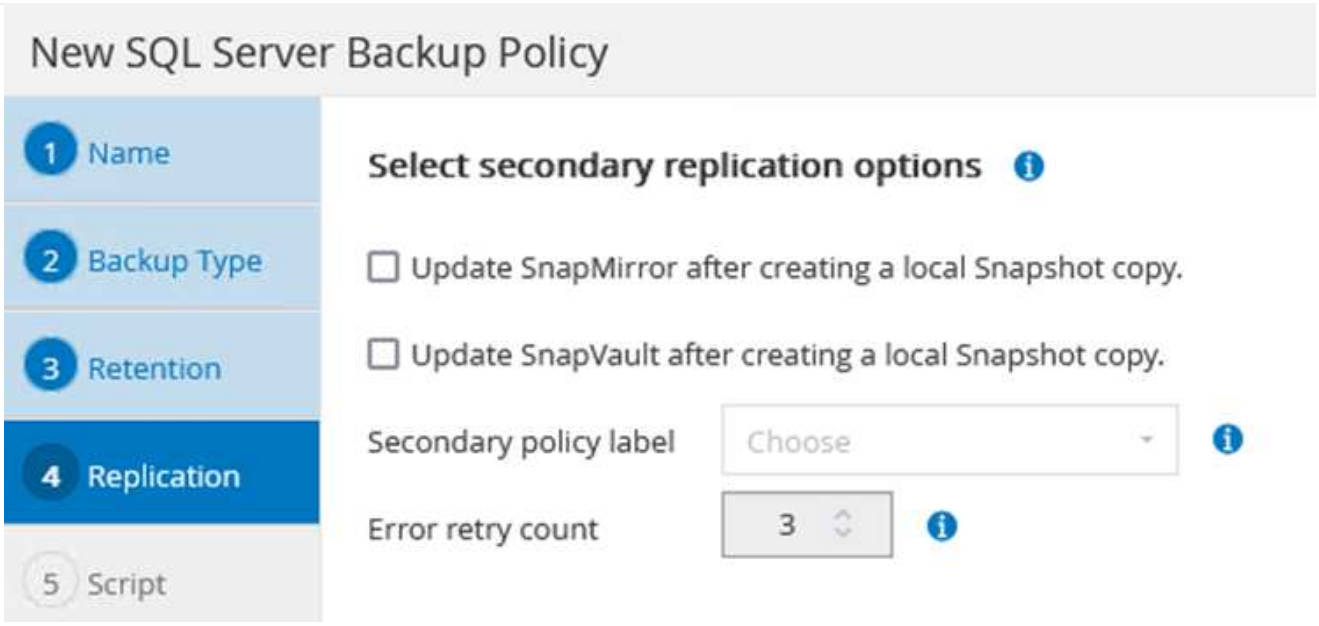
SQL Serverバックアップのポリシー作成の詳細については、 "SnapCenterのドキュメント" 。

Oracleバックアップのポリシー作成の詳細については、 "SnapCenterのドキュメント" 。

注記:

- ポリシー作成ウィザードを進める際には、レプリケーション セクションに特に注意してください。このセクションでは、バックアップ プロセス中に取得するセカンダリSnapMirrorコピーの種類を指定します。
- 「ローカル Snapshot コピーの作成後にSnapMirrorを更新する」設定は、同じクラスタに存在する 2 つのストレージ仮想マシン間にSnapMirror関係が存在する場合に、その関係を更新することを指します。
- 「ローカル SnapShot コピーの作成後にSnapVault を更新する」設定は、2 つの別個のクラスター間、およびオンプレミスのONTAPシステムとCloud Volumes ONTAPまたは FSx ONTAP間に存在するSnapMirror関係を更新するために使用されます。

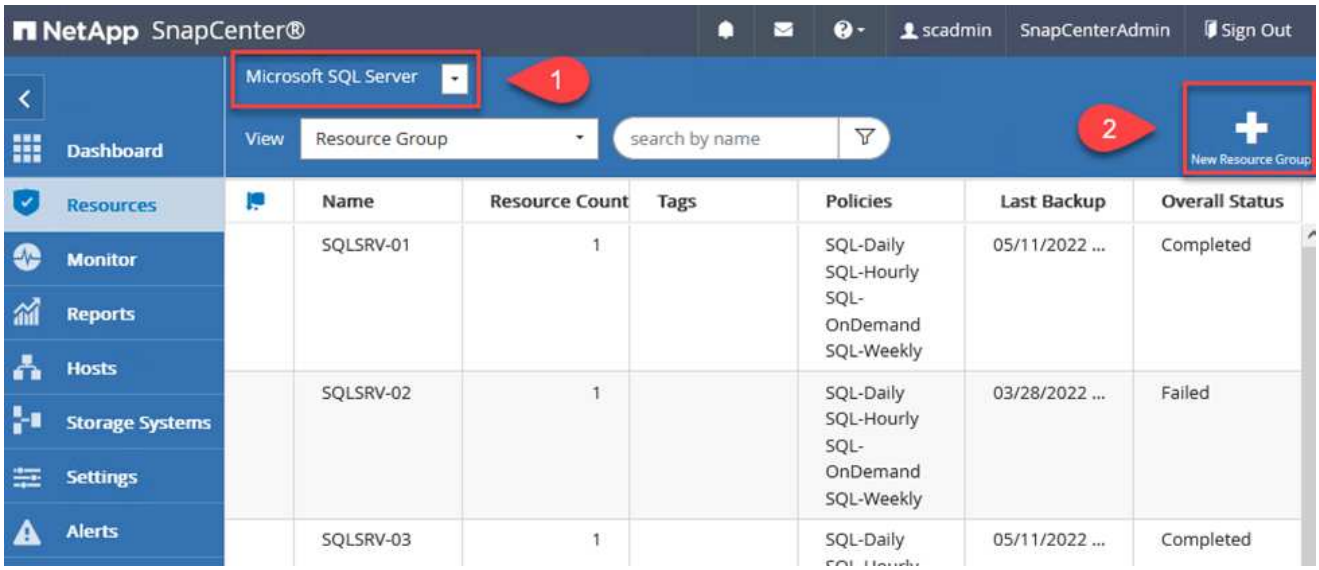
次の画像は、上記のオプションと、それらがバックアップ ポリシー ウィザードでどのように表示されるかを示しています。



SnapCenterリソース グループを作成する

リソース グループを使用すると、バックアップに含めるデータベース リソースと、それらのリソースに適用するポリシーを選択できます。

1. 左側のメニューの「リソース」セクションに移動します。
2. ウィンドウの上部で、操作するリソース タイプ (この場合は Microsoft SQL Server) を選択し、[新しいリソース グループ] をクリックします。



SnapCenter のドキュメントでは、SQL Server と Oracle データベースの両方のリソース グループを作成する手順が詳細に説明されています。

SQLリソースをバックアップするには、 "このリンク" 。

Oracleリソースのバックアップについては、 "このリンク" 。

Veeam バックアップ サーバーの導入と構成

このソリューションでは、Veeam Backup & Replication ソフトウェアを使用してアプリケーション仮想マシンをバックアップし、Veeam スケールアウト バックアップ リポジトリ (SOBR) を使用してバックアップのコピーを Amazon S3 バケットにアーカイブします。このソリューションでは、Veeam は Windows サーバーに展開されます。 Veeamの導入に関する具体的なガイダンスについては、 "Veeamヘルプセンター 技術ドキュメント" 。

Veeamスケールアウトバックアップリポジトリを構成する

ソフトウェアを展開してライセンスを取得したら、バックアップ ジョブのターゲット ストレージとしてスケールアウト バックアップ リポジトリ (SOBR) を作成できます。また、災害復旧のために VM データのオフサイト バックアップとして S3 バケットも含める必要があります。

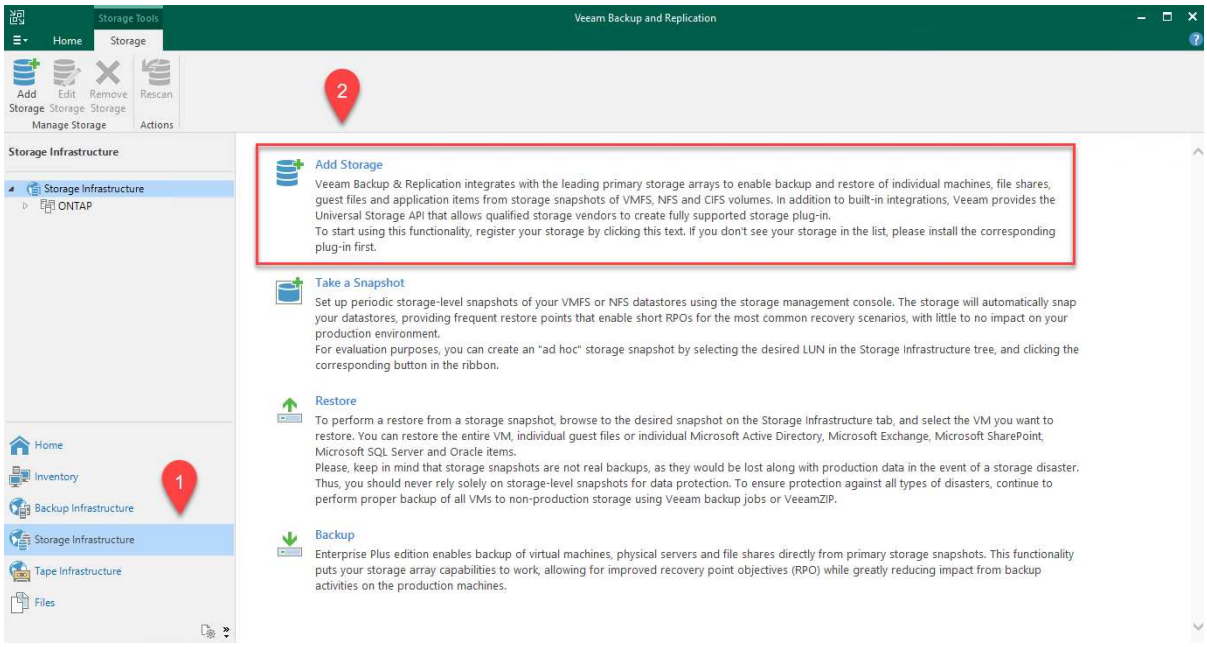
始める前に次の前提条件を確認してください。

1. オンプレミスのONTAPシステムに、バックアップのターゲット ストレージとして SMB ファイル共有を作成します。
2. SOBR に含める Amazon S3 バケットを作成します。これはオフサイト バックアップのリポジトリです。

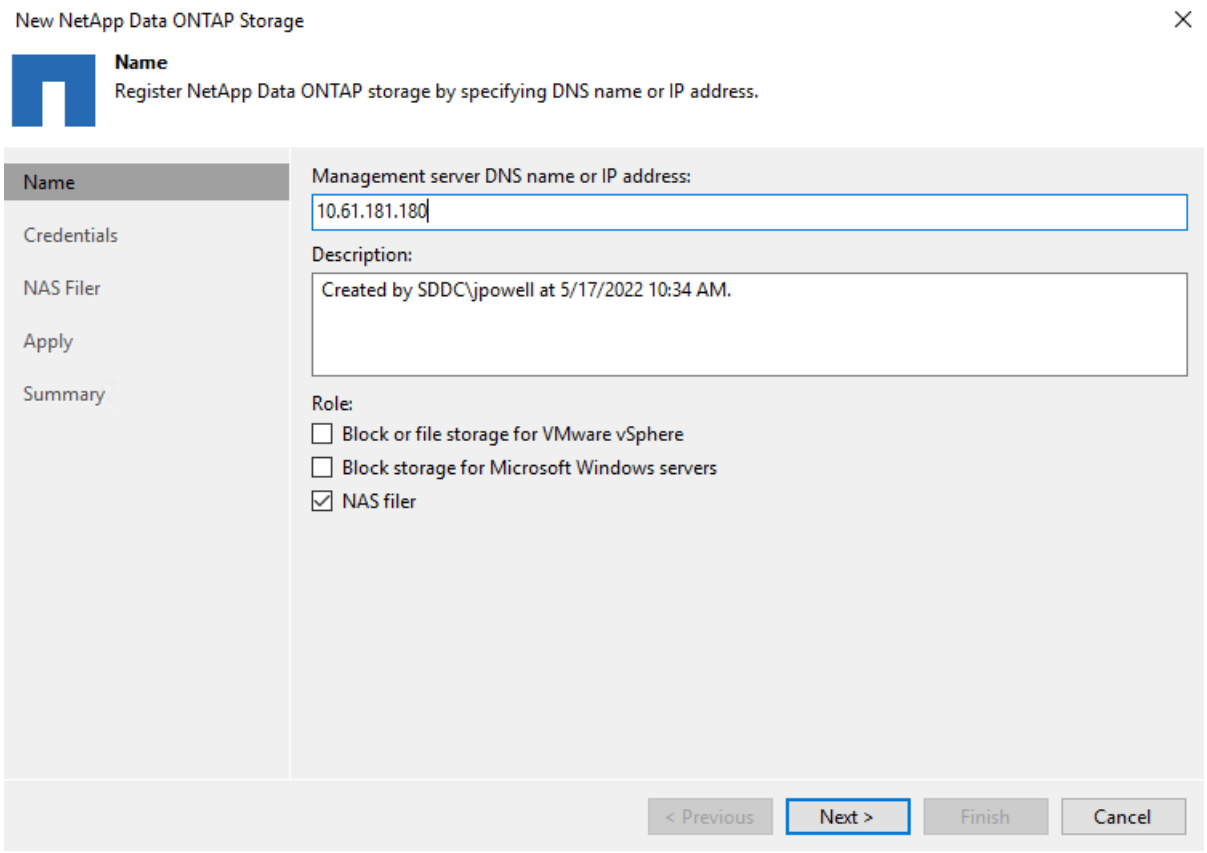
VeeamにONTAPストレージを追加

まず、 ONTAPストレージ クラスターと関連する SMB/NFS ファイルシステムを Veeam のストレージ インフラストラクチャとして追加します。

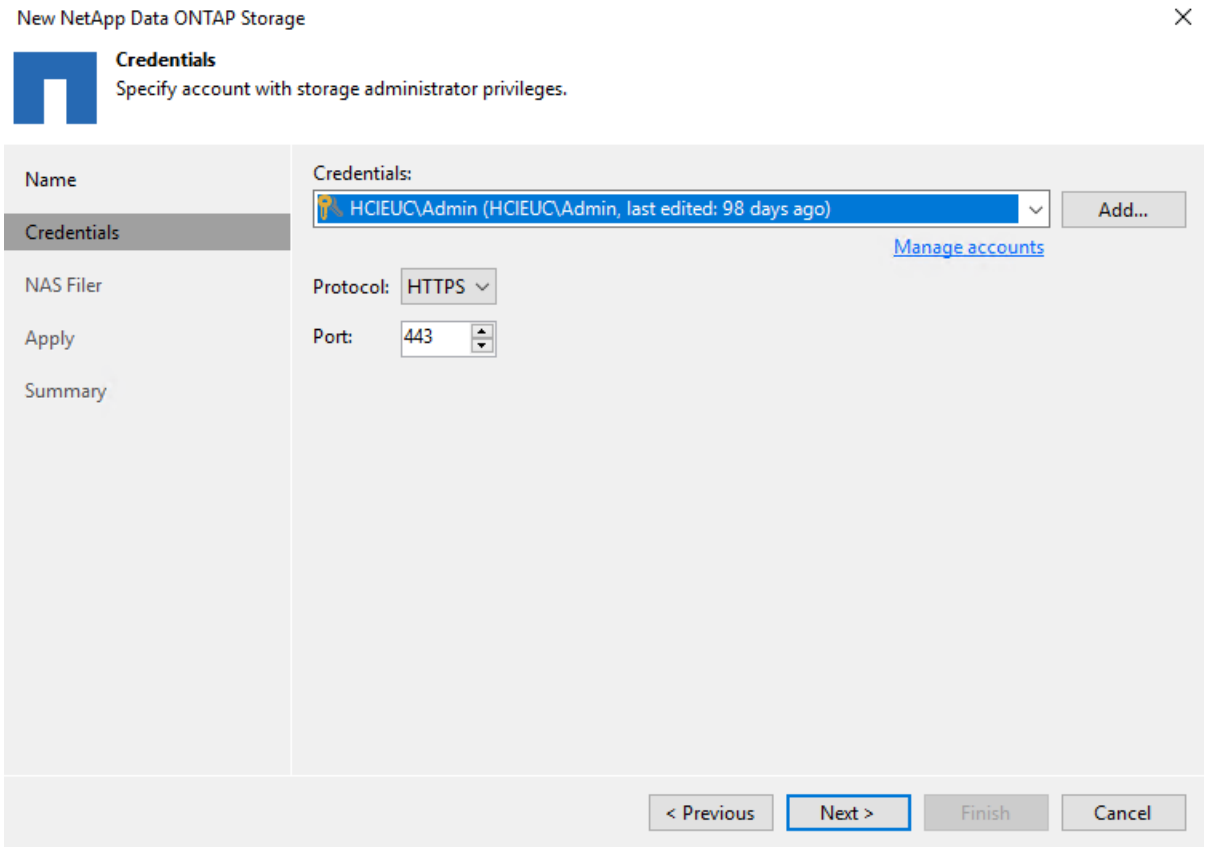
1. Veeam コンソールを開いてログインします。「ストレージ インフラストラクチャ」に移動し、「ストレージの追加」を選択します。



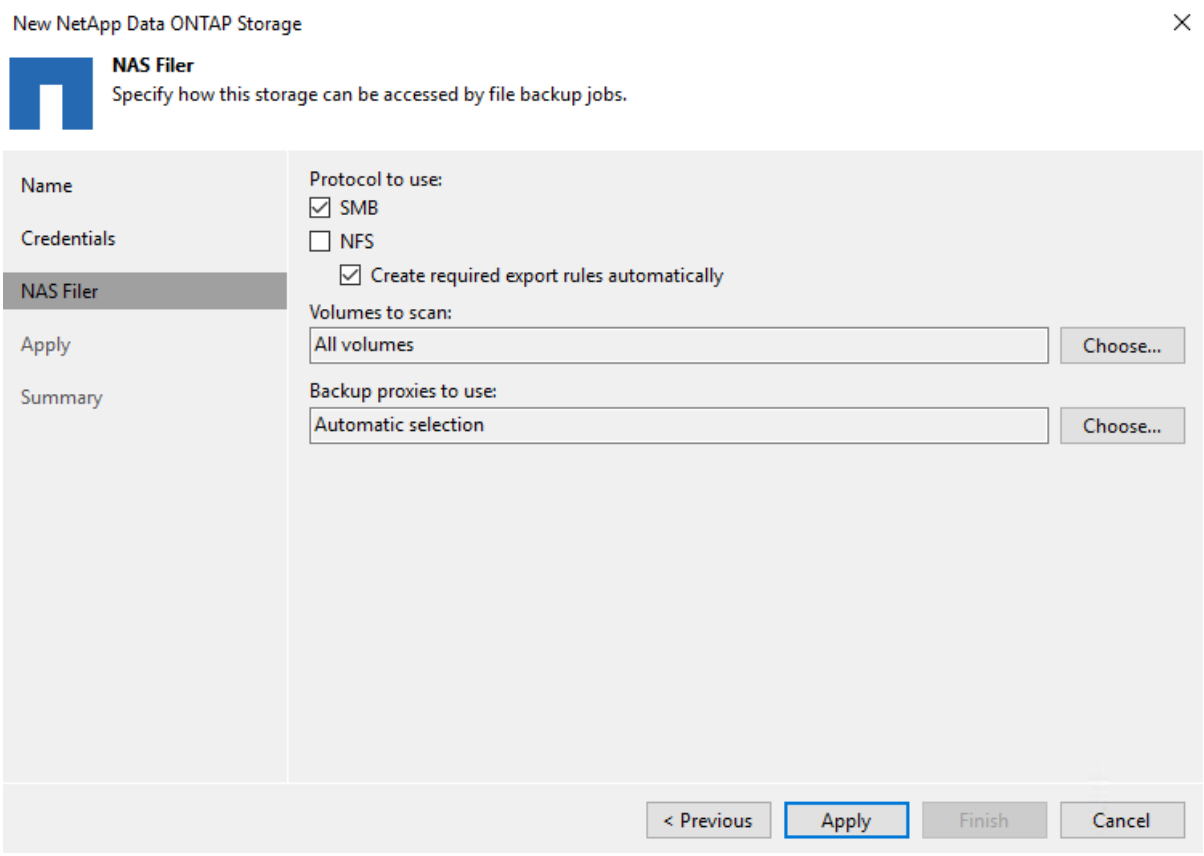
2. ストレージの追加ウィザードで、ストレージ ベンダーとしてNetAppを選択し、 Data ONTAPを選択します。
3. 管理 IP アドレスを入力し、NAS Filer ボックスをオンにします。[Next]をクリックします。



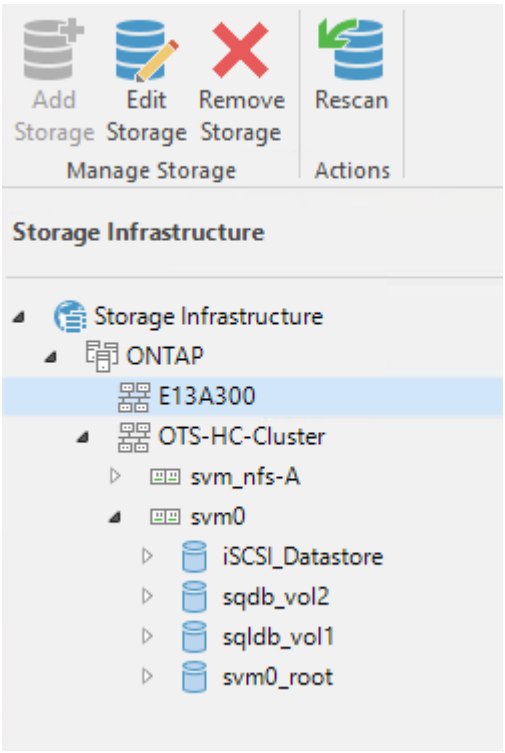
4. ONTAPクラスターにアクセスするための資格情報を追加します。



5. NAS Filer ページで、スキャンするプロトコルを選択し、「次へ」を選択します。

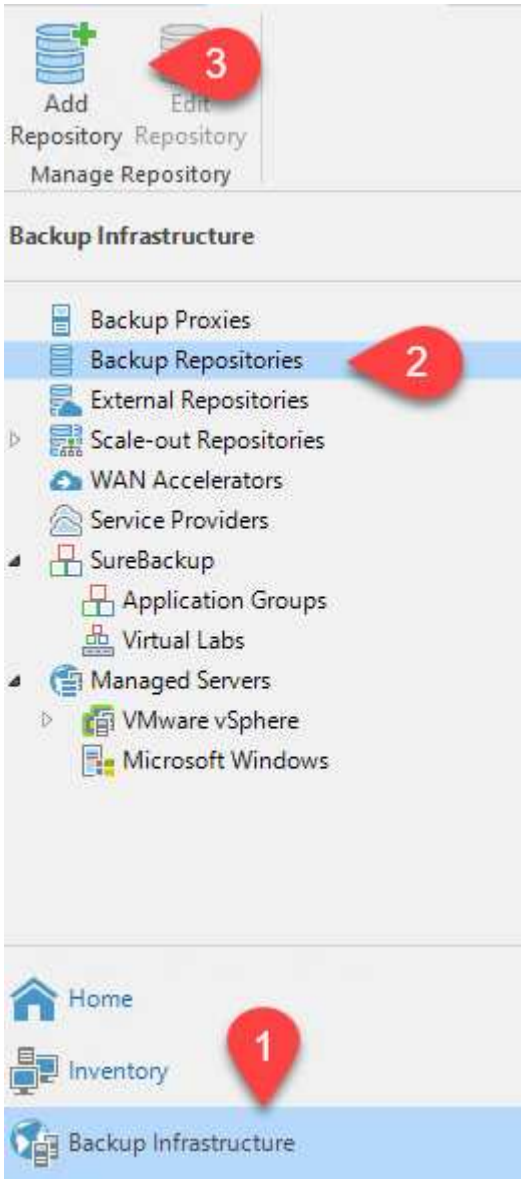


6. ウィザードの [適用] ページと [概要] ページを完了し、[完了] をクリックしてストレージ検出プロセスを開始します。スキャンが完了すると、 ONTAPクラスターが NAS ファイラーとともに使用可能なリソースとして追加されます。

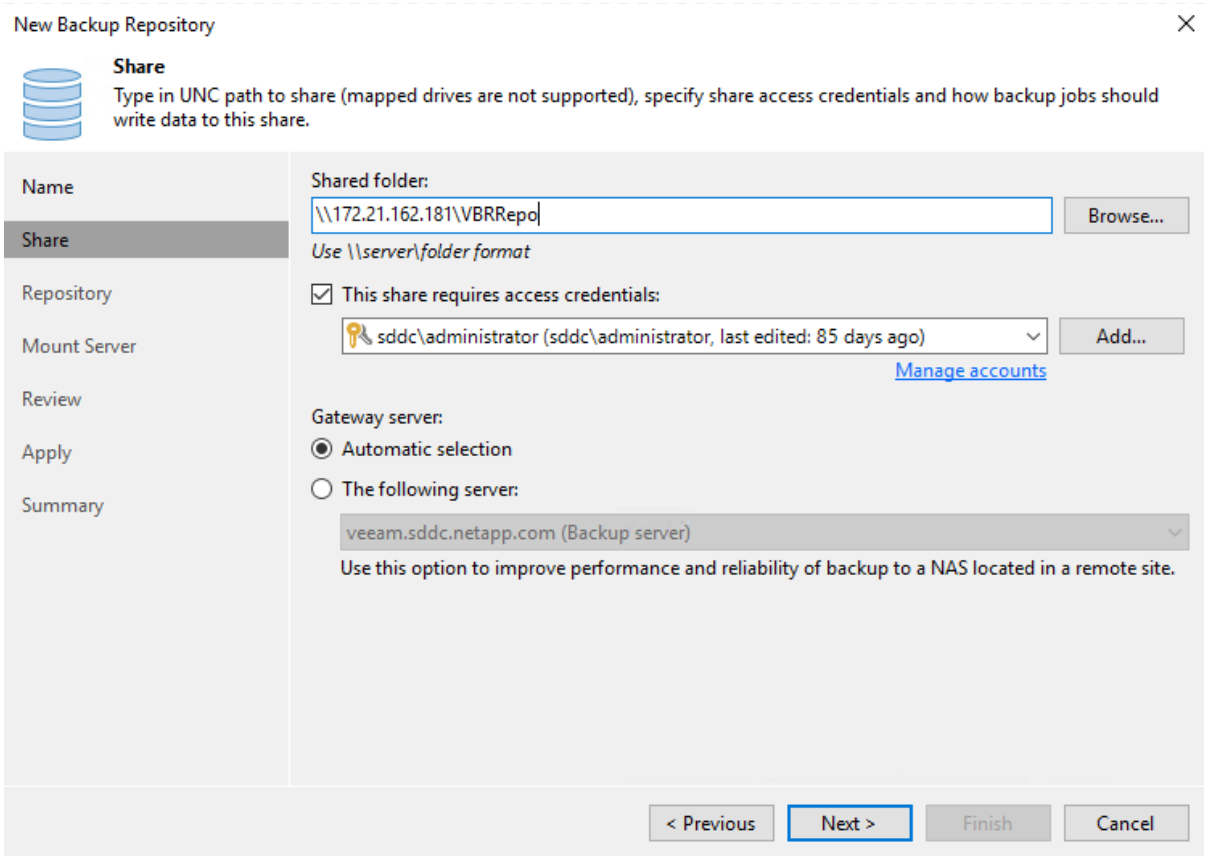


7. 新しく検出された NAS 共有を使用してバックアップ リポジトリを作成します。バックアップ インフラストラクチャから、バックアップ リポジトリを選択し、リポジトリの追加メニュー項

目をクリックします。



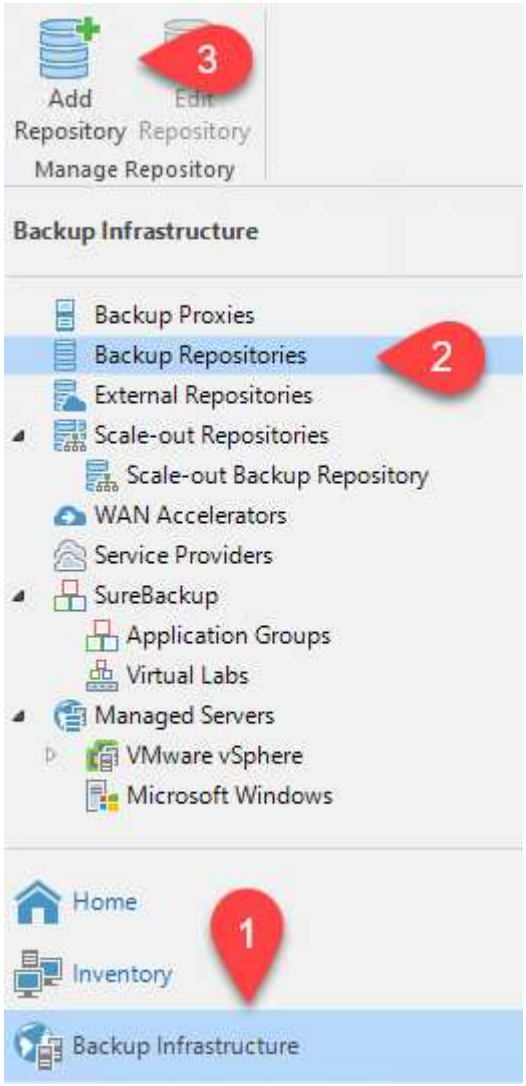
8. 新しいバックアップ リポジトリ ウィザードのすべての手順に従ってリポジトリを作成します。Veeamバックアップリポジトリの作成の詳細については、 "Veeamのドキュメント" 。


New Backup Repository
Share
Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.
Name
Share
Repository
Mount Server
Review
Apply
Summary
Shared folder:
\\172.21.162.181\VBRRepo
Browse...
Use \\server\folder format
This share requires access credentials:
sddc\administrator (sddc\administrator, last edited: 85 days ago)
Add...
Manage accounts
Gateway server:
Automatic selection
The following server:
veeam.sddc.netapp.com (Backup server)
Use this option to improve performance and reliability of backup to a NAS located in a remote site.
< Previous
Next >
Finish
Cancel

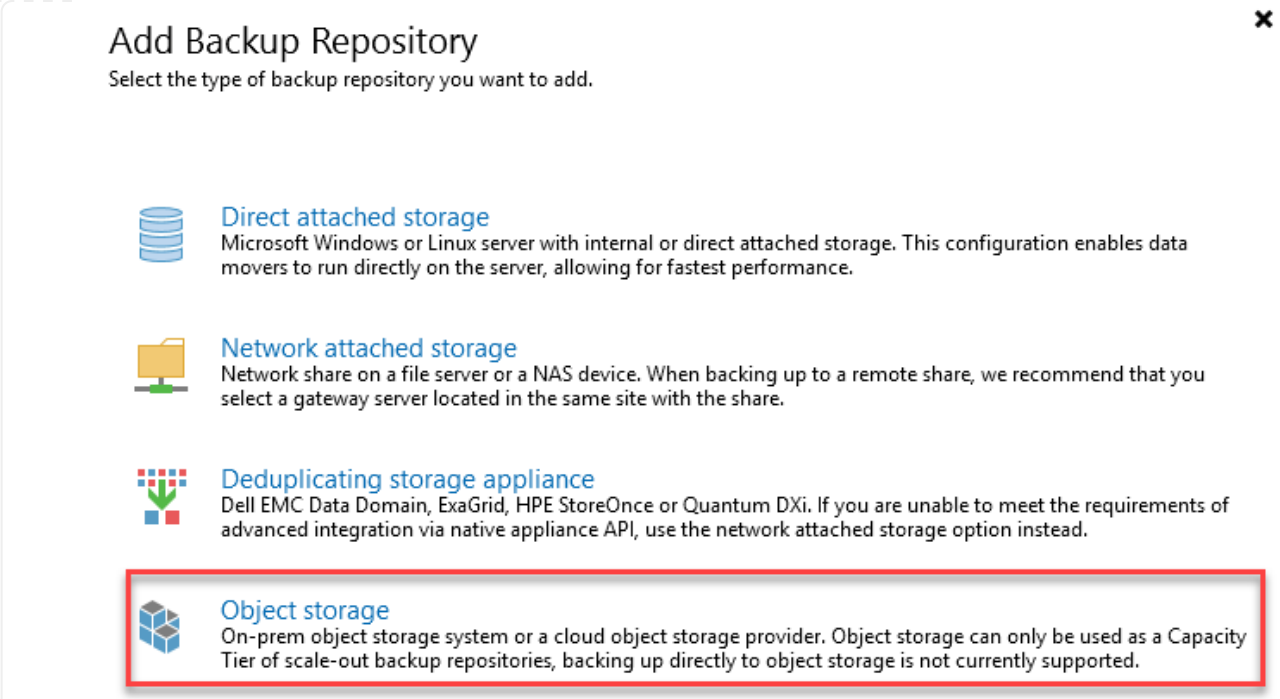
Amazon S3 バケットをバックアップリポジトリとして追加する

次のステップは、Amazon S3 ストレージをバックアップ リポジトリとして追加することです。

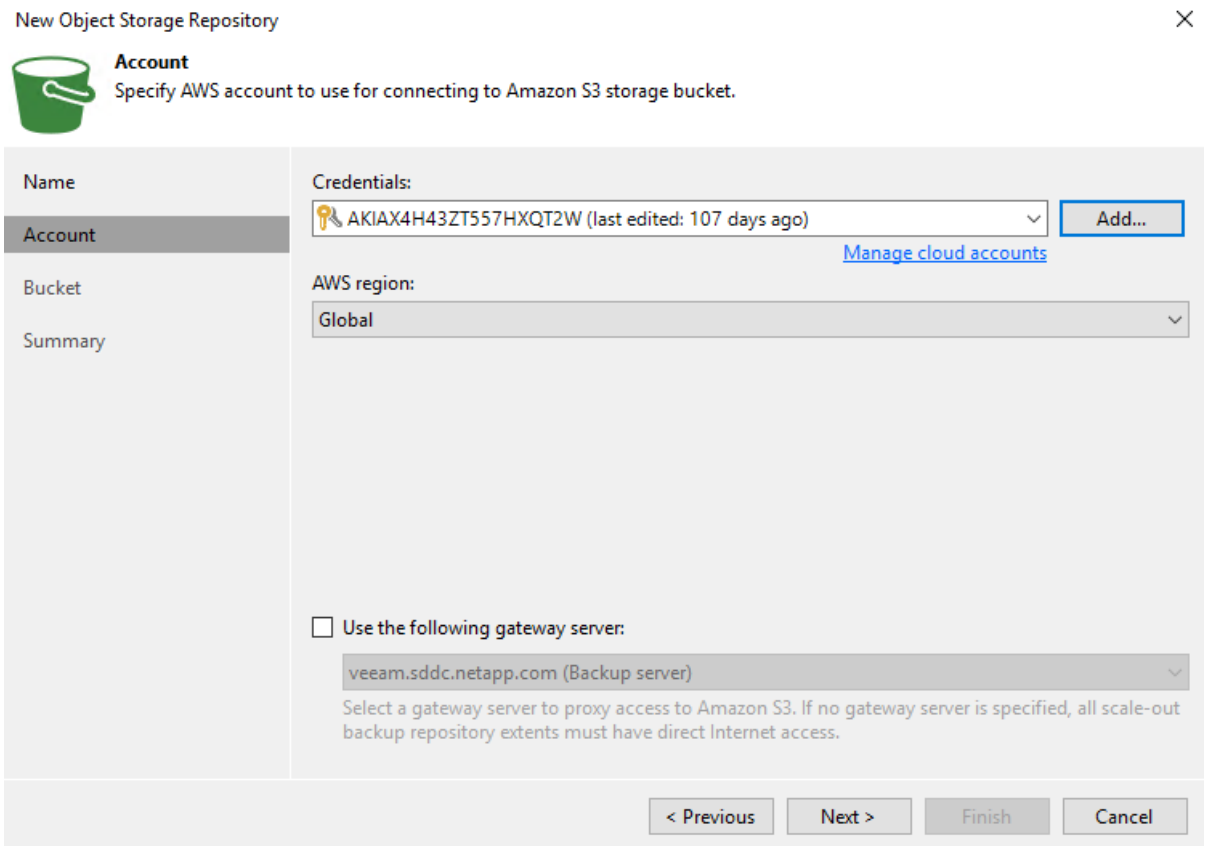
1. [バックアップ インフラストラクチャ] > [バックアップ リポジトリ] に移動します。リポジトリの追加をクリックします。



2. バックアップ リポジトリの追加ウィザードで、オブジェクト ストレージを選択し、Amazon S3 を選択します。これにより、新しいオブジェクト ストレージ リポジトリ ウィザードが起動します。



3. オブジェクト ストレージ リポジトリの名前を指定して、「次へ」をクリックします。
4. 次のセクションで、資格情報を入力します。 AWS アクセスキーとシークレットキーが必要です。

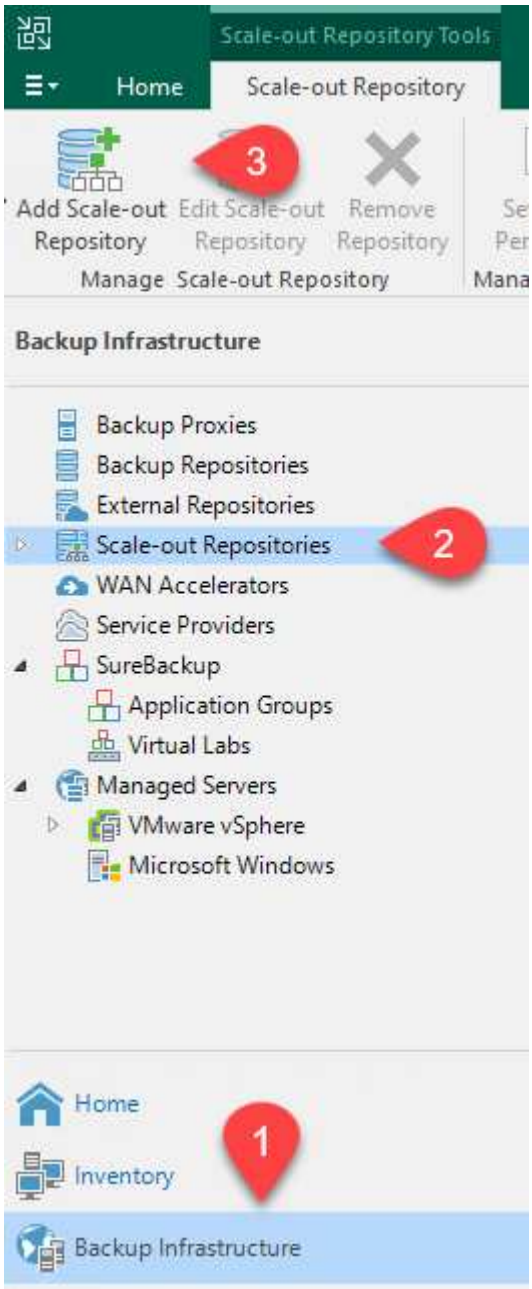


5. Amazon 構成が読み込まれたら、データセンター、バケット、フォルダーを選択し、「適用」をクリックします。最後に、「完了」をクリックしてウィザードを終了します。

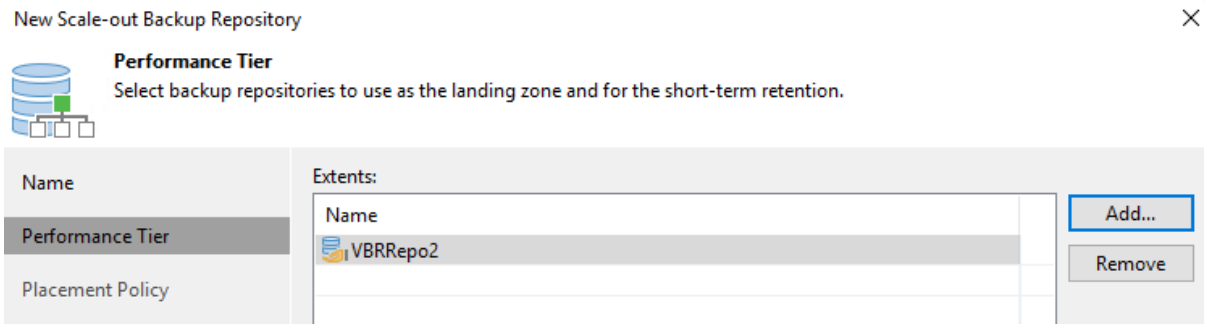
スケールアウトバックアップリポジトリを作成する

ストレージ リポジトリを Veeam に追加したので、災害復旧のためにオフサイトの Amazon S3 オブジェクト ストレージにバックアップ コピーを自動的に階層化する SOBR を作成できます。

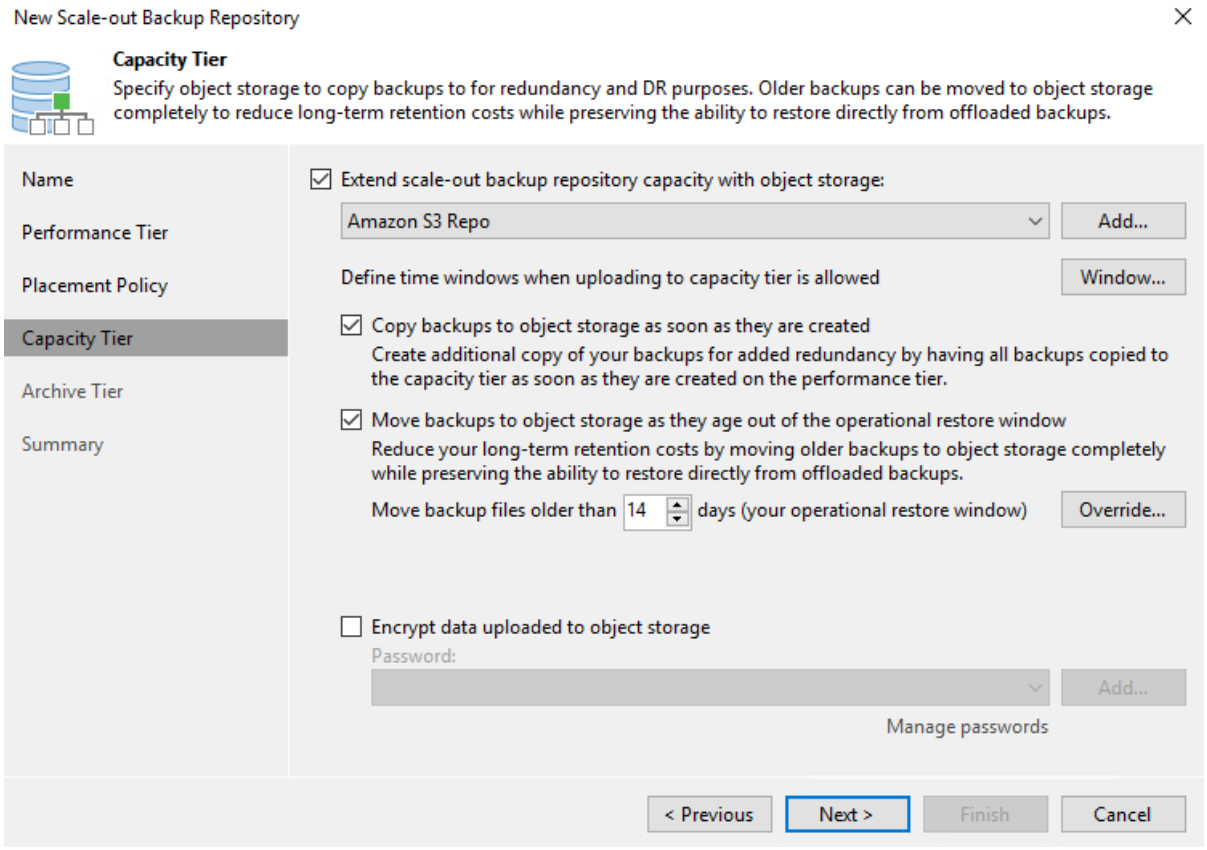
1. バックアップ インフラストラクチャから、スケールアウト リポジトリを選択し、スケールアウト リポジトリの追加メニュー項目をクリックします。



2. 新しいスケールアウト バックアップ リポジトリで SOBR の名前を入力し、[次へ] をクリックします。
3. パフォーマンス層では、ローカルONTAPクラスタにある SMB 共有を含むバックアップ リポジトリを選択します。



4. 配置ポリシーでは、要件に基づいてデータのローカリティまたはパフォーマンスのいずれかを選択します。次へを選択します。
5. 容量層では、Amazon S3 オブジェクト ストレージを使用して SOBR を拡張します。災害復旧のために、セカンダリ バックアップがタイムリーに配信されるように、[バックアップが作成されたらすぐにオブジェクト ストレージにコピーする] を選択します。



6. 最後に、「適用」と「完了」を選択して、SOBR の作成を完了します。

スケールアウトバックアップリポジトリジョブを作成する

Veeam を構成する最後の手順は、新しく作成された SOBR をバックアップ先として使用してバックアップ ジョブを作成することです。バックアップ ジョブの作成は、ストレージ管理者の通常の業務の一部であるため、ここでは詳細な手順については説明しません。 Veeamでのバックアップジョブ作成の詳細については、 "Veeamヘルプセンター技術ドキュメント" 。

BlueXP backup and recoveryツールと構成

AWS で実行されている VMware Cloud Volumes サービスへのアプリケーション VM とデータベース ボリュームのフェイルオーバーを実行するには、 SnapCenter Server と Veeam Backup and Replication Server の両方の実行中のインスタンスをインストールして構成する必要があります。フェールオーバーが完了したら、オンプレミスのデータセンターへのフェールバックが計画され実行されるまで、通常のバックアップ操作を再開するようにこれらのツールを構成する必要もあります。

セカンダリ **Windows SnapCenter Server** を展開する

SnapCenter Server は、VMware Cloud SDDC にデプロイされるか、VMware Cloud 環境にネットワーク接続された VPC にある EC2 インスタンスにインストールされます。

SnapCenter softwareはNetAppサポート サイトから入手でき、ドメインまたはワークグループ内に存在する Microsoft Windows システムにインストールできます。詳細な計画ガイドとインストール手順については、 "NetAppドキュメント センター" 。

SnapCenter softwareは次の場所にあります。 "このリンク" 。

セカンダリ **Windows SnapCenter Server** を構成する

FSx ONTAPにミラーリングされたアプリケーション データの復元を実行するには、まずオンプレミスのSnapCenterデータベースの完全復元を実行する必要があります。このプロセスが完了すると、VM との通信が再確立され、FSx ONTAP をプライマリ ストレージとして使用してアプリケーションのバックアップを再開できるようになります。

これを実現するには、 SnapCenterサーバーで次の項目を完了する必要があります。

1. コンピューター名を元のオンプレミスのSnapCenter Server と同じになるように構成します。
2. VMware Cloud および FSx ONTAPインスタンスと通信するためのネットワークを構成します。
3. SnapCenterデータベースを復元する手順を完了します。
4. SnapCenterがディザスタ リカバリ モードになっていることを確認して、FSx がバックアップのプライマリ ストレージになっていることを確認します。
5. 復元された仮想マシンとの通信が再確立されたことを確認します。

セカンダリ**Veeam Backup & Replication**サーバーを導入する

Veeam Backup & Replication サーバーは、VMware Cloud on AWS 内の Windows サーバーまたは EC2 インスタンスにインストールできます。詳細な実装ガイダンスについては、 "Veeamヘルプセンター技術ドキュメント" 。

セカンダリ **Veeam Backup & Replication** サーバーを構成する

Amazon S3 ストレージにバックアップされた仮想マシンの復元を実行するには、Windows サーバーに Veeam Server をインストールし、VMware Cloud、FSx ONTAP、および元のバックアップ リポジトリを含む S3 バケットと通信するように構成する必要があります。また、VM を復元した後に新しいバックアップを実行するには、FSx ONTAPに新しいバックアップ リポジトリを構成する必要があります。

このプロセスを実行するには、次の項目を完了する必要があります。

1. VMware Cloud、FSx ONTAP、および元のバックアップ リポジトリを含む S3 バケットと通信するようにネットワークを構成します。
2. FSx ONTAP上の SMB 共有を新しいバックアップ リポジトリとして構成します。
3. オンプレミスのスケールアウト バックアップ リポジトリの一部として使用されていた元の S3 バケットをマウントします。
4. VM を復元した後、SQL VM と Oracle VM を保護するための新しいバックアップ ジョブを確立します。

Veeamを使用したVMの復元の詳細については、セクションを参照してください。"Veeam Full Restore でアプリケーション VM を復元する" 。

災害復旧のための**SnapCenter**データベースバックアップ

SnapCenter、災害発生時にSnapCenterサーバーを復旧できるように、基盤となる MySQL データベースと構成データのバックアップと復旧が可能です。私たちのソリューションでは、VPC にある AWS EC2 インスタンス上のSnapCenterデータベースと構成を復元しました。 SnapCenterの災害復旧の詳細については、以下を参照してください。 "このリンク" 。

SnapCenterバックアップの前提条件

SnapCenterバックアップには次の前提条件が必要です。

- バックアップされたデータベースと構成ファイルを見つけるためにオンプレミスのONTAPシステム上に作成されたボリュームと SMB 共有。
- オンプレミスのONTAPシステムと AWS アカウントの FSx または CVO 間のSnapMirror関係。この関係は、バックアップされたSnapCenterデータベースと構成ファイルを含むスナップショットを転送するために使用されます。
- EC2 インスタンスまたは VMware Cloud SDDC 内の VM のいずれかのクラウド アカウントにインストールされた Windows Server。
- VMware Cloud の Windows EC2 インスタンスまたは VM にインストールされたSnapCenter 。

SnapCenter のバックアップと復元プロセスの概要

- バックアップ db および構成ファイルをホストするためのボリュームをオンプレミスのONTAPシステムに作成します。
- オンプレミスと FSx/CVO の間にSnapMirror関係を設定します。
- SMB 共有をマウントします。
- API タスクを実行するための Swagger 認証トークンを取得します。
- db 復元プロセスを開始します。
- xcopy ユーティリティを使用して、db および config ファイルのローカル ディレクトリを SMB 共有にコピーします。
- FSx で、 ONTAPボリュームのクローンを作成します (オンプレミスからSnapMirror経由でコピーされます)。
- FSx から EC2/VMware Cloud に SMB 共有をマウントします。
- 復元ディレクトリを SMB 共有からローカル ディレクトリにコピーします。
- Swagger から SQL Server の復元プロセスを実行します。

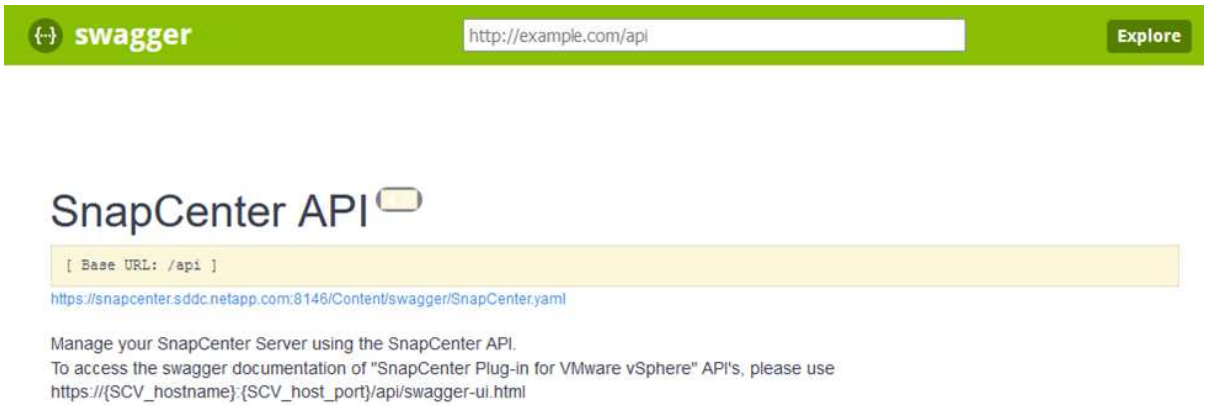
SnapCenterデータベースと構成をバックアップする

SnapCenter は、REST API コマンドを実行するための Web クライアント インターフェイスを提供します。 Swaggerを介してREST APIにアクセスする方法については、 SnapCenterのドキュメントを参照してください。 "このリンク" 。

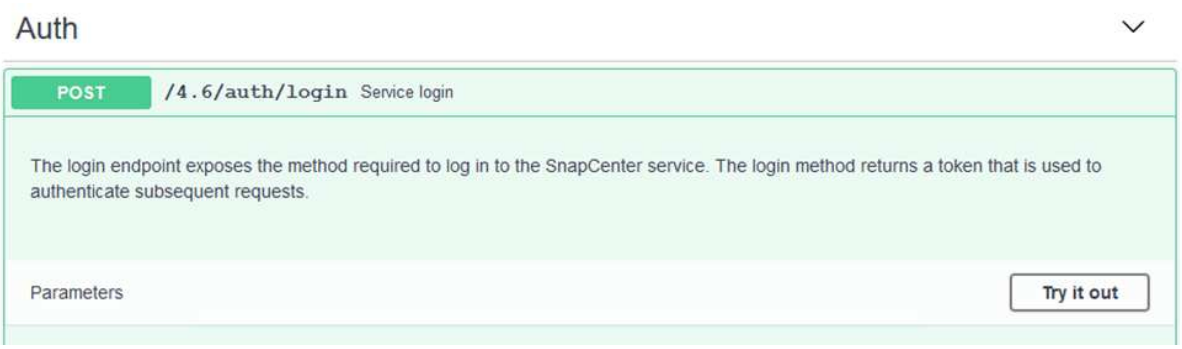
Swaggerにログインして認証トークンを取得する

Swagger ページに移動した後、データベース復元プロセスを開始するために認証トークンを取得する必要があります。

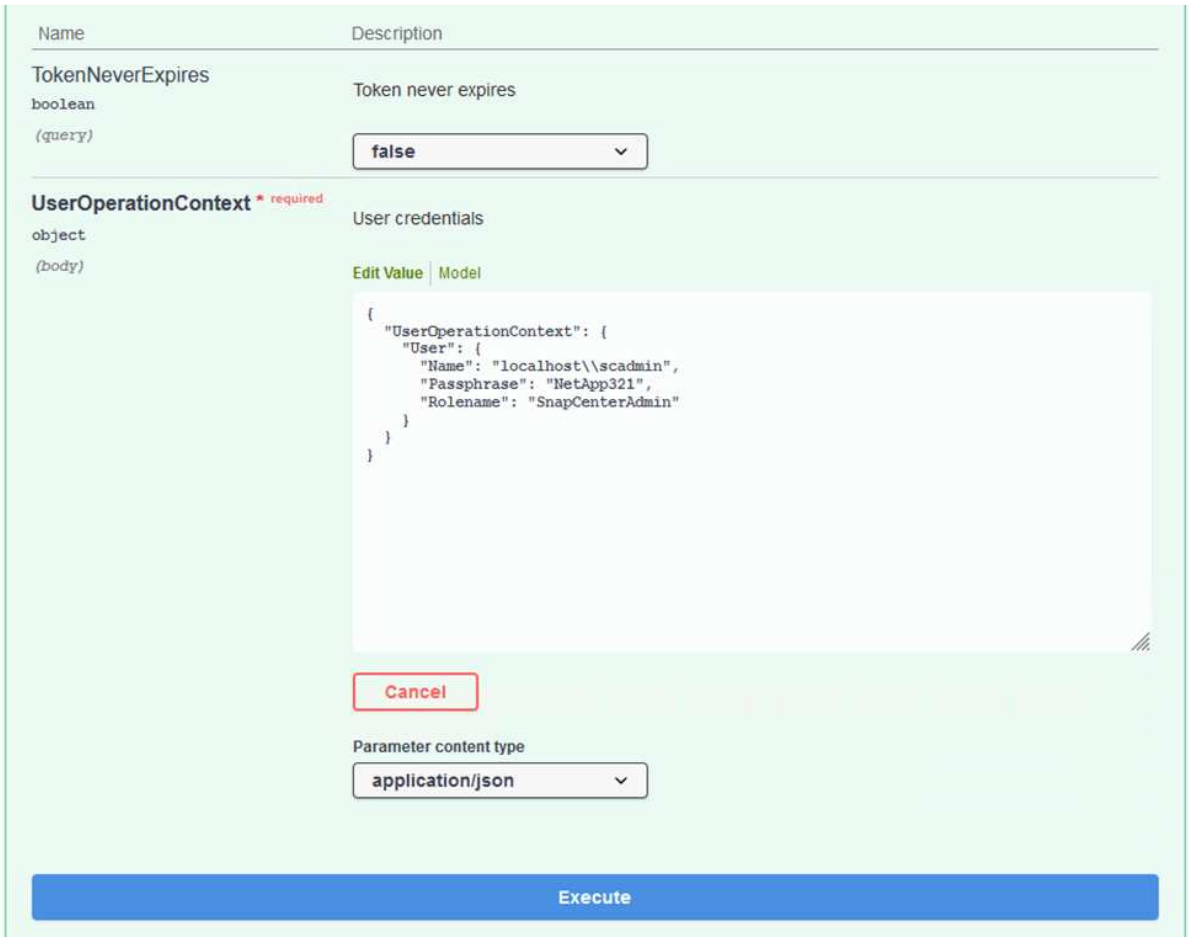
1. *https://< SnapCenter Server IP>:8146/swagger/* にあるSnapCenter Swagger API Web ページにアクセスします。



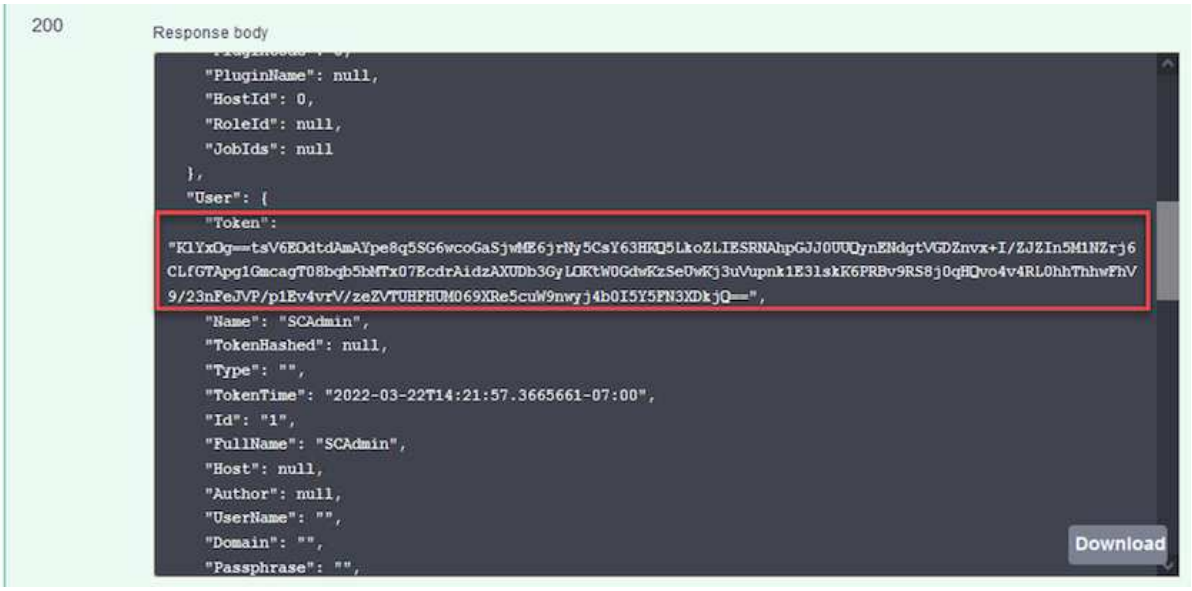
2. 認証セクションを展開し、「試してみる」をクリックします。



3. UserOperationContext 領域で、 SnapCenter の資格情報とロールを入力し、[実行] をクリックします。



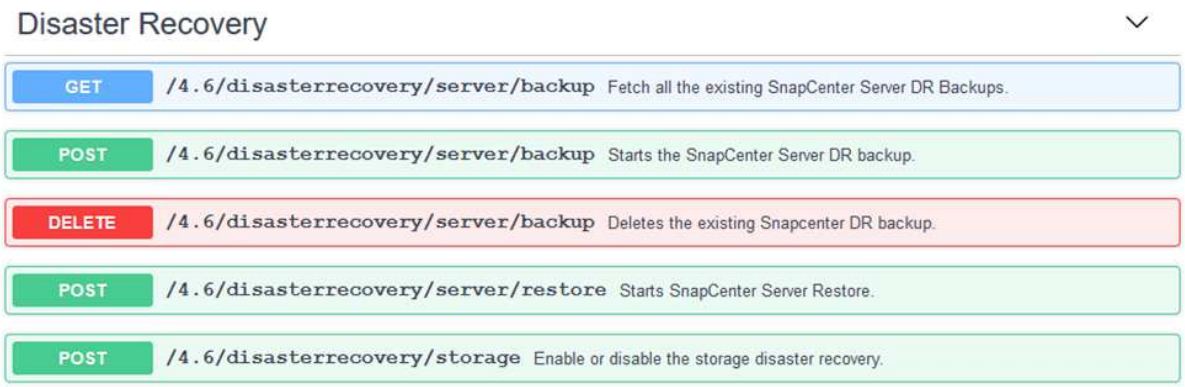
4. 以下のレスポンス本文でトークンを確認できます。バックアッププロセスを実行するときに、認証用のトークンテキストをコピーします。



SnapCenterデータベースのバックアップを実行する

次に、Swagger ページの Disaster Recovery 領域に移動して、 SnapCenterバックアップ プロセスを開始します。

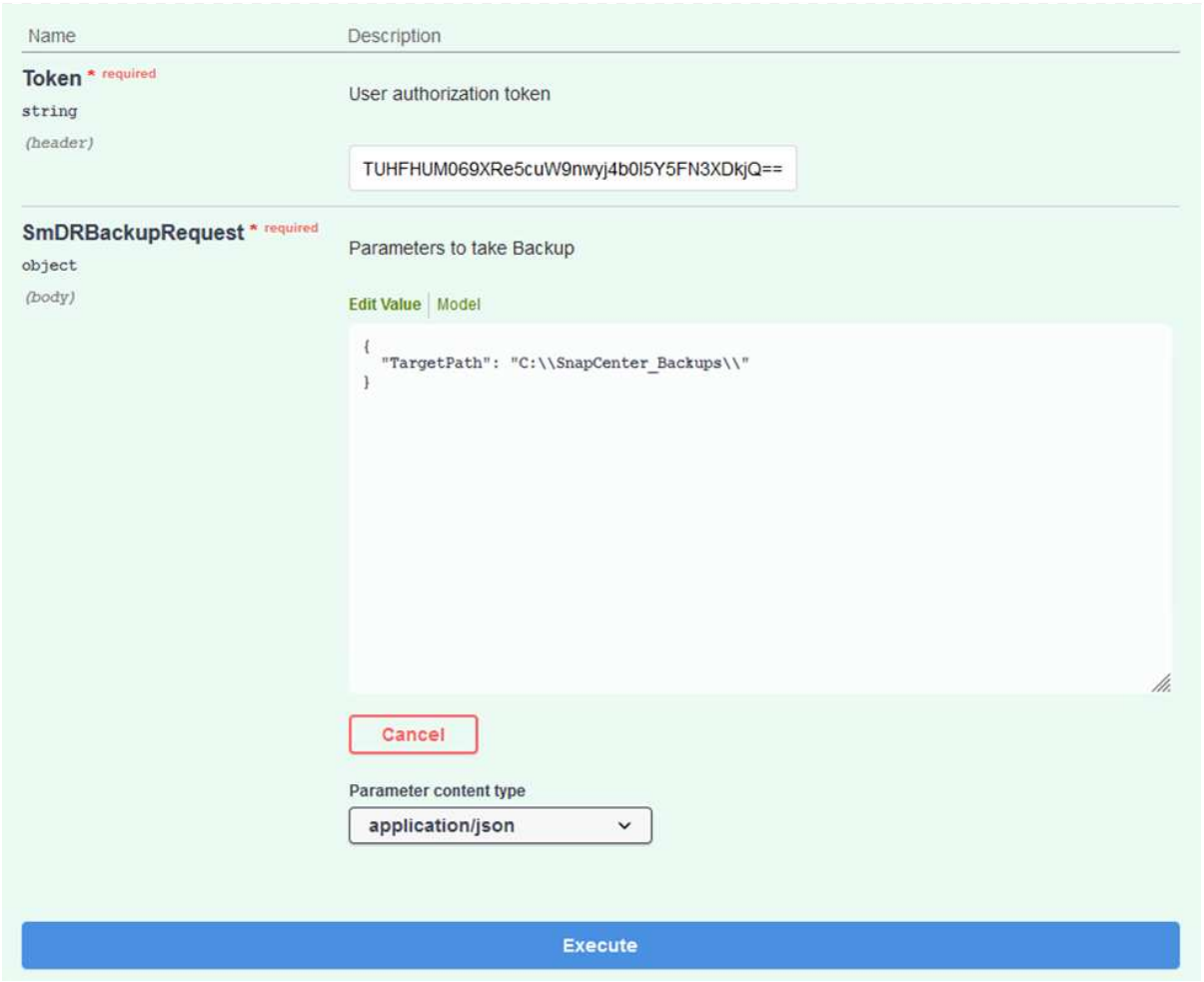
1. 災害復旧領域をクリックして展開します。



2. 拡大する `/4.6/disasterrecovery/server/backup`セクションにアクセスし、[試してみる] をクリックします。

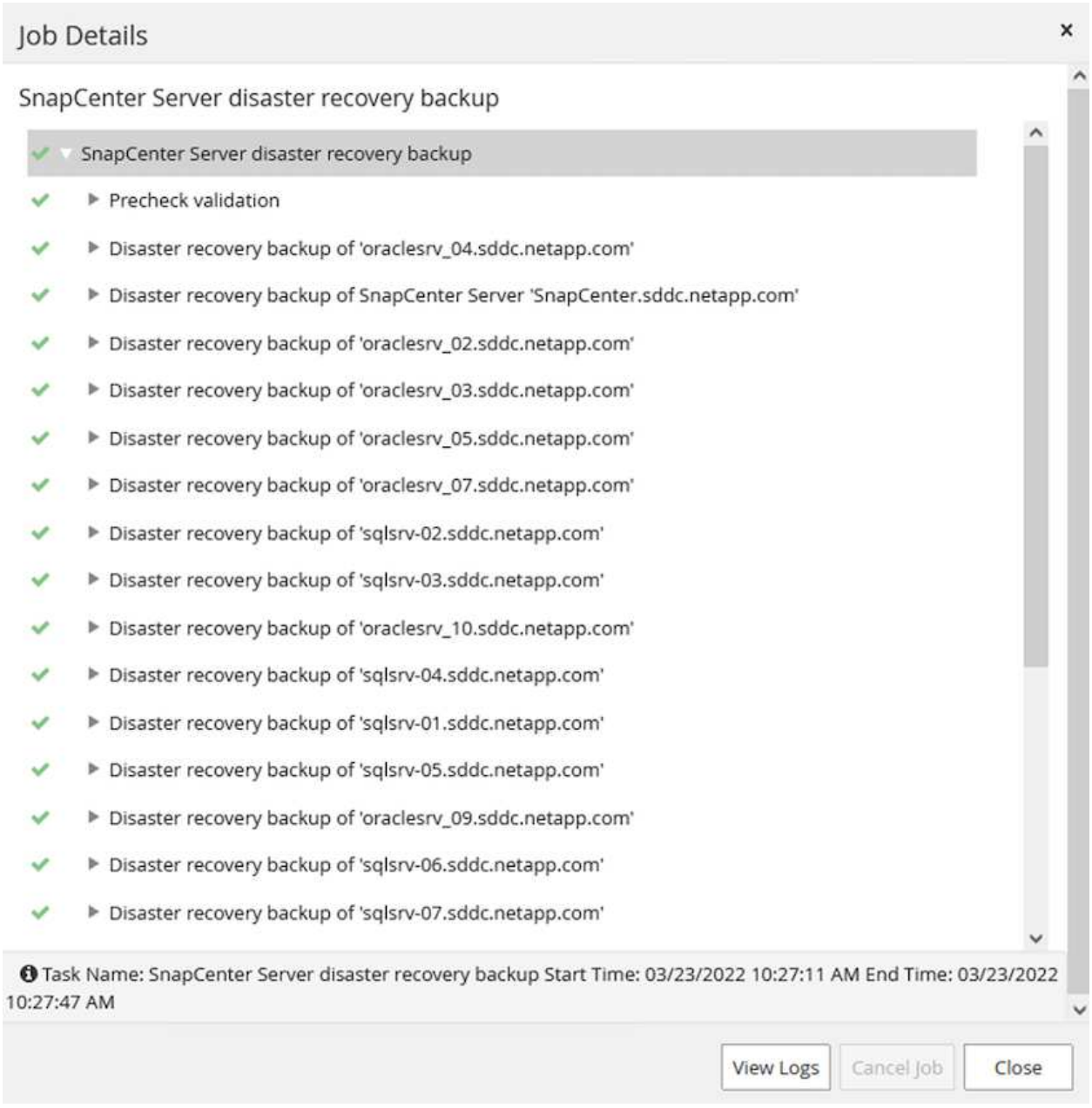
3. SmDRBackupRequest セクションで、正しいローカル ターゲット パスを追加し、[実行] を選択してSnapCenterデータベースと構成のバックアップを開始します。

> バックアップ プロセスでは、NFS または CIFS ファイル共有に直接バックアップすることはできません。


Name
Description
Token * required
string
(header)
User authorization token
TUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ==
SmDRBackupRequest * required
object
(body)
Parameters to take Backup
Edit Value
Model
{
"TargetPath": "C:\\SnapCenter_Backups\\"
}
Cancel
Parameter content type
application/json
Execute

SnapCenterからバックアップジョブを監視する

データベースの復元プロセスを開始するときは、 SnapCenterにログインしてログ ファイルを確認します。 [モニター] セクションでは、 SnapCenterサーバーの災害復旧バックアップの詳細を表示できます。



XCOPYユーティリティを使用して、データベースのバックアップファイルを**SMB**共有にコピーします。

次に、 SnapCenterサーバー上のローカル ドライブから、AWS の FSx インスタンスにあるセカンダリ ロケーションにデータをSnapMirrorコピーするために使用される CIFS 共有にバックアップを移動する必要があります。ファイルの権限を保持する特定のオプションを指定して xcopy を使用します。

管理者としてコマンドプロンプトを開きます。コマンドプロンプトから次のコマンドを入力します。

```
xcopy  <Source_Path>  \\<Destination_Server_IP>\<Folder_Path> /O /X
/E /H /K
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O
/X /E /H /K
```

フェイルオーバー

プライマリサイトで災害が発生

プライマリオンプレミスデータセンターで災害が発生した場合、VMware Cloud on AWS を使用して Amazon Web Services インフラストラクチャにあるセカンダリサイトへのフェイルオーバーがシナリオに含まれます。仮想マシンとオンプレミスのONTAPクラスターにはアクセスできなくなっていると想定します。さらに、 SnapCenterと Veeam の両方の仮想マシンにアクセスできなくなり、セカンダリ サイトで再構築する必要があります。

このセクションでは、インフラストラクチャのクラウドへのフェイルオーバーについて説明し、次のトピックを取り上げます。

- SnapCenterデータベースの復元。新しいSnapCenterサーバーが確立されたら、MySQL データベースと構成ファイルを復元し、データベースを災害復旧モードに切り替えて、セカンダリ FSx ストレージがプライマリ ストレージ デバイスになることができるようにします。
- Veeam Backup & Replication を使用してアプリケーション仮想マシンを復元します。 VM バックアップが含まれている S3 ストレージを接続し、バックアップをインポートして、VMware Cloud on AWS に復元します。
- SnapCenterを使用して SQL Server アプリケーション データを復元します。
- SnapCenterを使用して Oracle アプリケーション データを復元します。

SnapCenterデータベースの復元プロセス

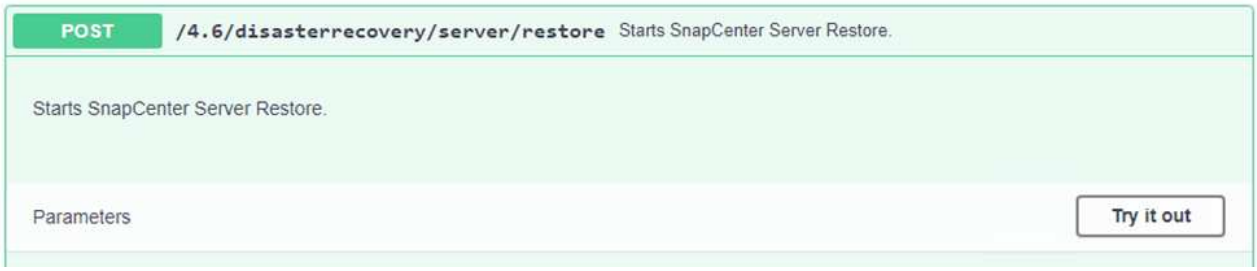
SnapCenter は、MySQL データベースと構成ファイルのバックアップと復元を可能にすることで、災害復旧シナリオをサポートします。これにより、管理者はオンプレミス データセンターでSnapCenterデータベースの定期的なバックアップを維持し、後でそのデータベースをセカンダリSnapCenterデータベースに復元できるようになります。

リモートSnapCenterサーバー上のSnapCenterバックアップ ファイルにアクセスするには、次の手順を実行します。

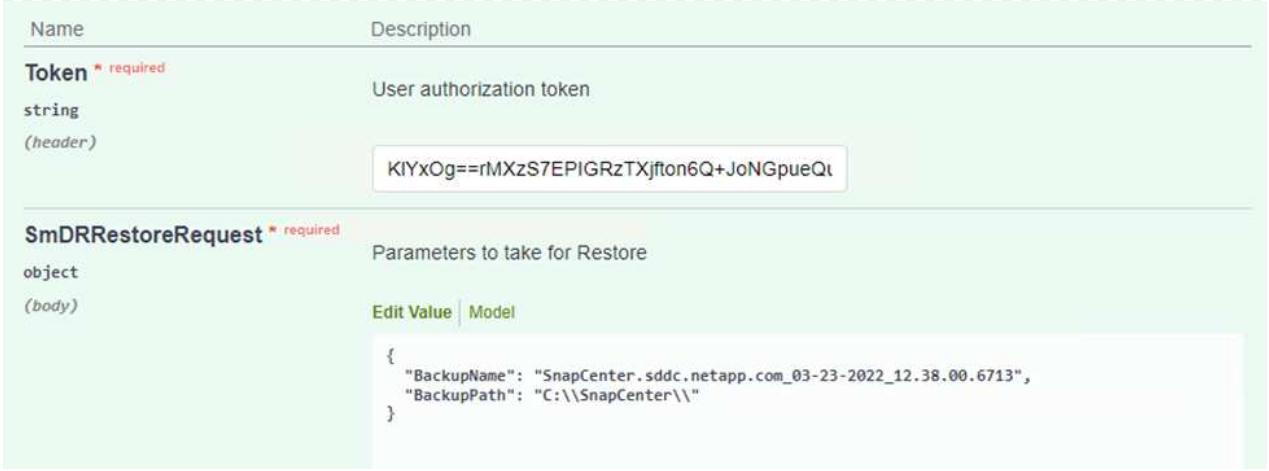
1. FSx クラスターからSnapMirror関係を解除し、ボリュームを読み取り/書き込み可能にします。
2. CIFS サーバーを作成し (必要な場合)、クローン ボリュームのジャンクション パスを指す CIFS 共有を作成します。
3. xcopy を使用して、バックアップ ファイルをセカンダリSnapCenterシステムのローカル ディレクトリにコピーします。
4. SnapCenter v4.6 をインストールします。
5. SnapCenterサーバーの FQDN が元のサーバーと同じであることを確認します。これは、DB の復元を成功させるために必要です。

復元プロセスを開始するには、次の手順を実行します。

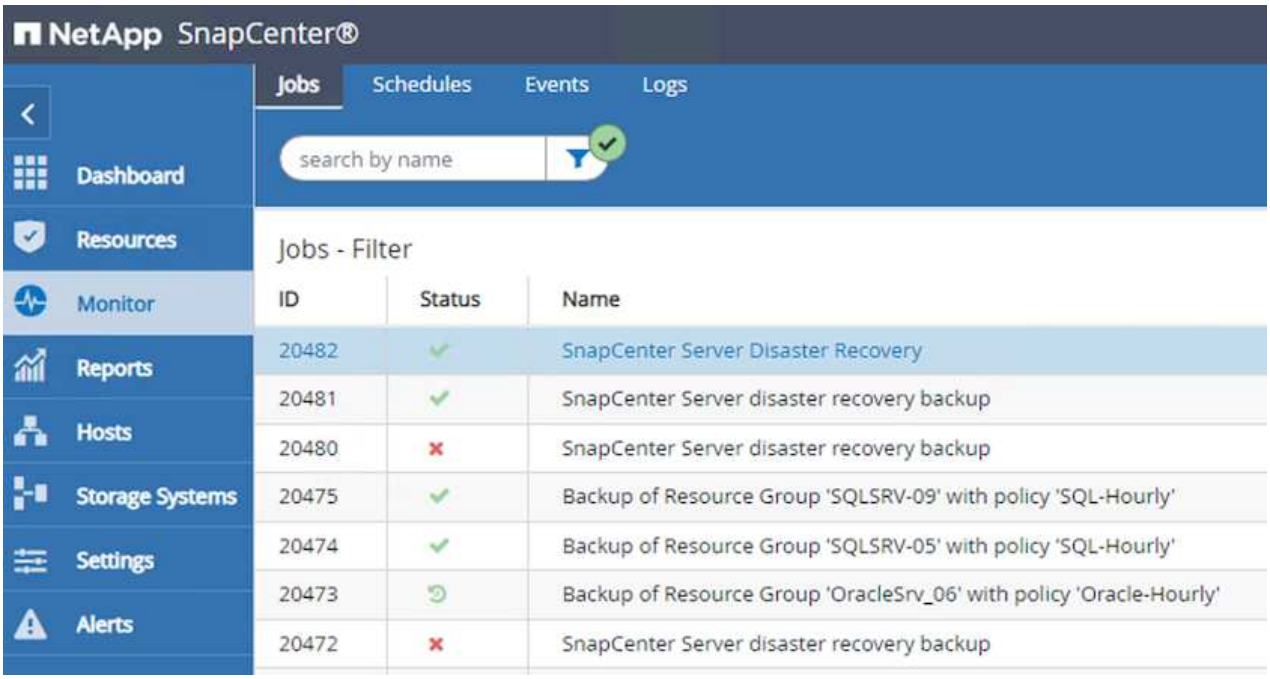
1. セカンダリSnapCenterサーバーの Swagger API Web ページに移動し、前の手順に従って認証トークンを取得します。
2. Swaggerページの災害復旧セクションに移動し、 `/4.6/disasterrecovery/server/restore`をクリックし、「試してみる」をクリックします。

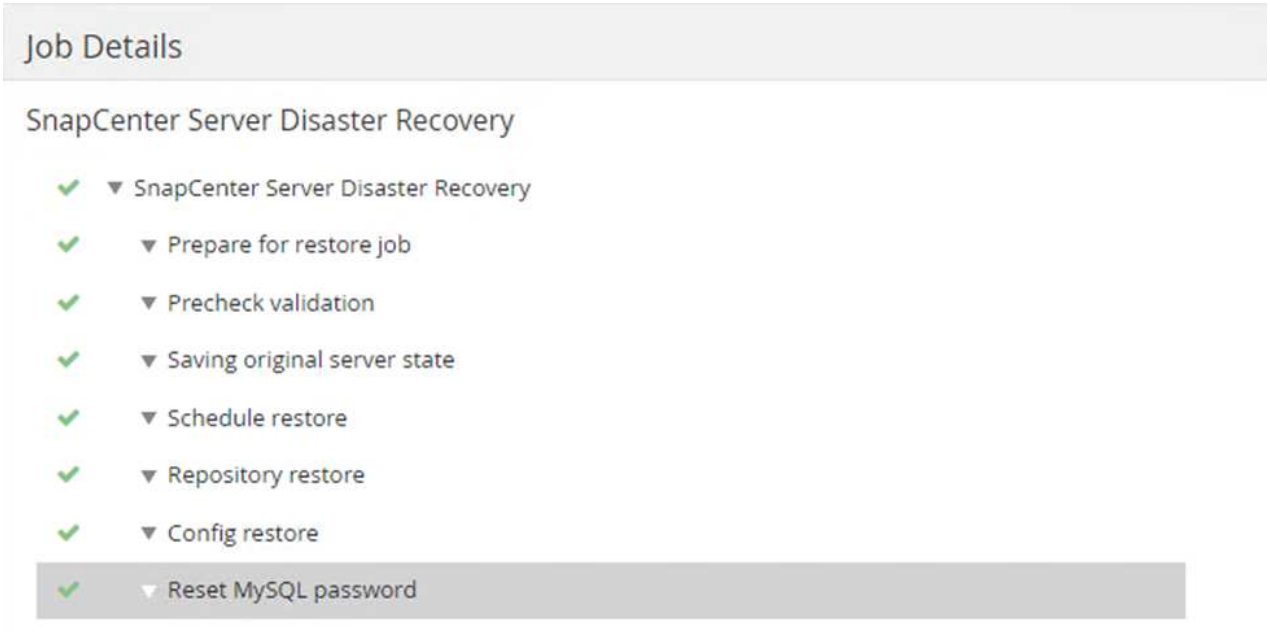


3. 認証トークンを貼り付け、SmDRResterRequest セクションにバックアップの名前とセカンダリSnapCenterサーバー上のローカル ディレクトリを貼り付けます。



4. 復元プロセスを開始するには、[実行] ボタンを選択します。
5. SnapCenterから [モニター] セクションに移動して、復元ジョブの進行状況を表示します。





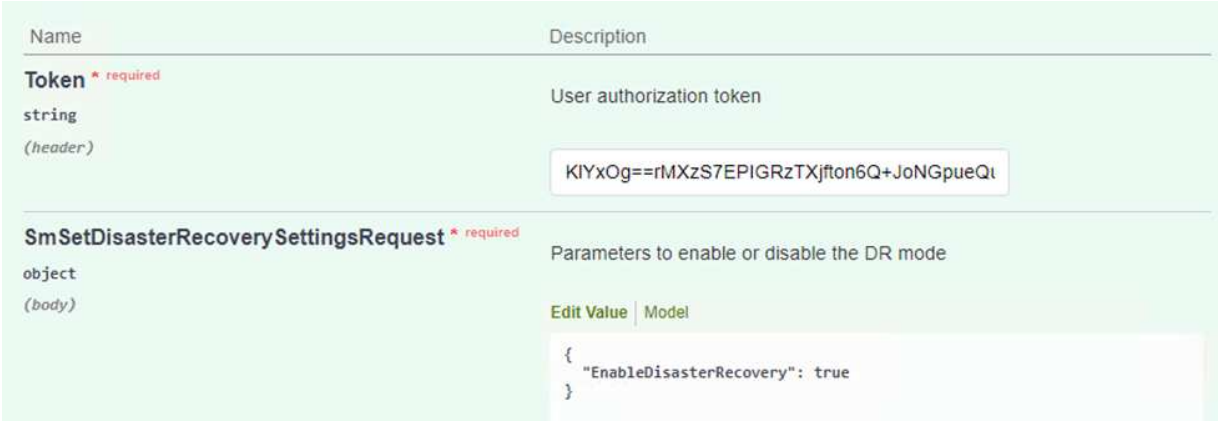
6. セカンダリ ストレージからの SQL Server の復元を有効にするには、 SnapCenterデータベースをディザスタ リカバリ モードに切り替える必要があります。これは個別の操作として実行され、Swagger API Web ページで開始されます。

   a. 災害復旧セクションに移動してクリックします `/4.6/disasterrecovery/storage`。

   b. ユーザー認証トークンを貼り付けます。

   c. SmSetDisasterRecoverySettingsRequestセクションで、変更します。 `EnableDisasterRecover`に `true`。

   d. [実行] をクリックして、SQL Server の災害復旧モードを有効にします。



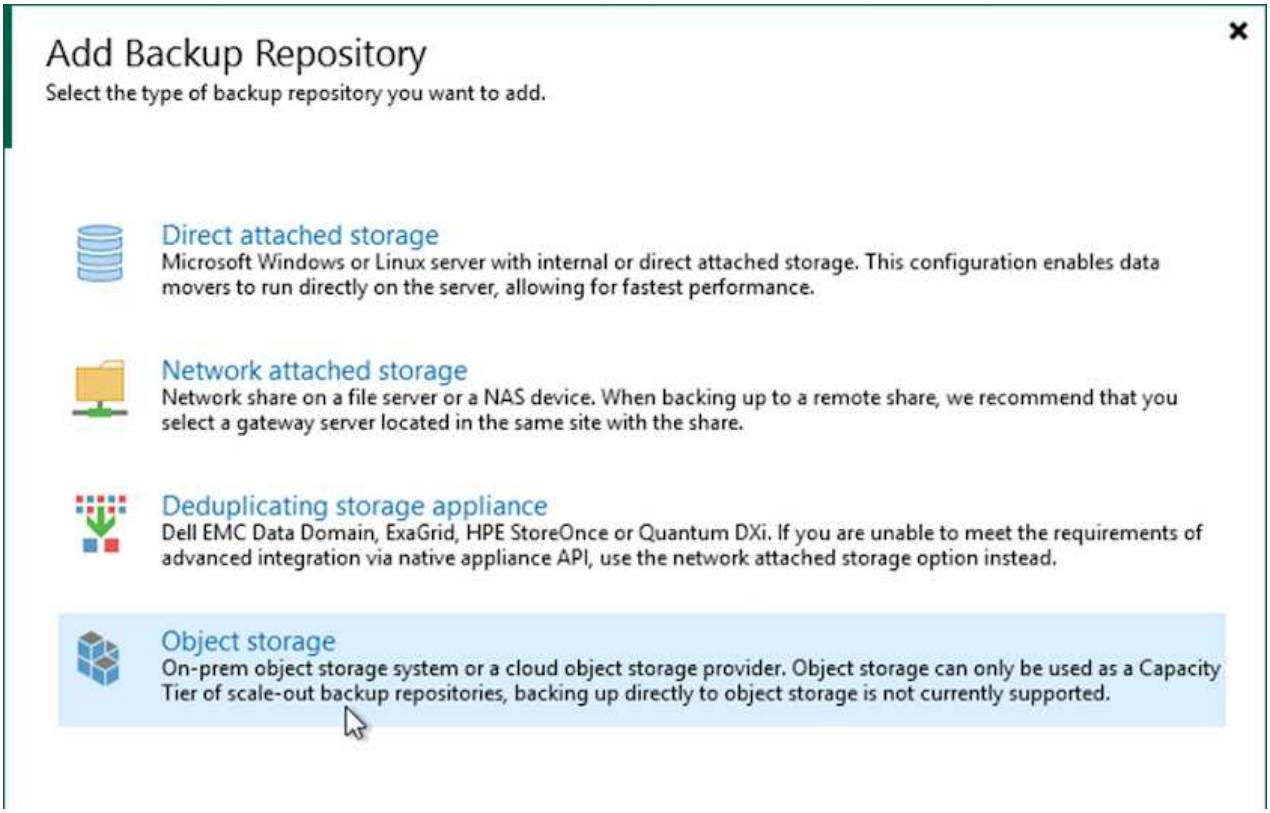
追加の手順に関するコメントを参照してください。

Veeam の完全復元でアプリケーション VM を復元する

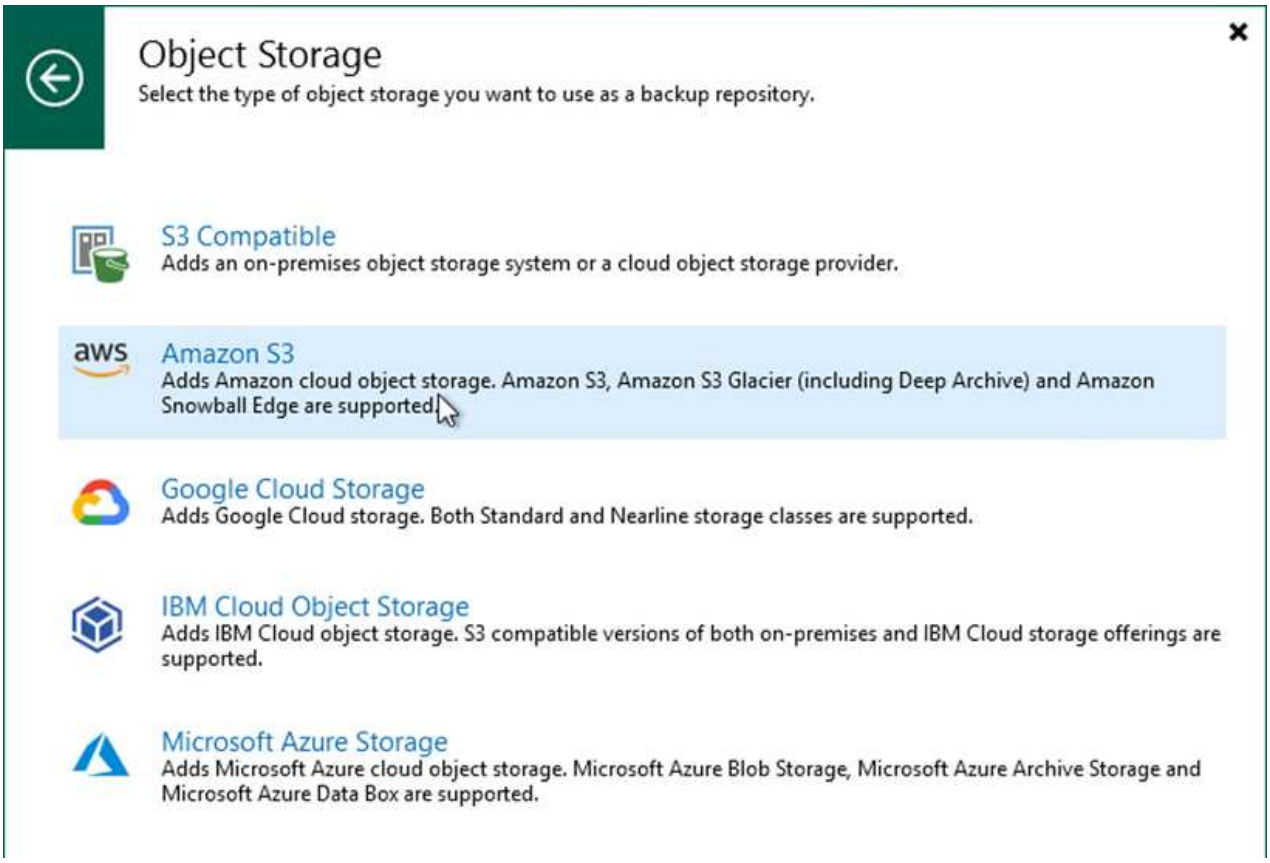
セカンダリ Veeam サーバーで、S3 ストレージからバックアップをインポートし、SQL Server および Oracle VM を VMware Cloud クラスターに復元します。

オンプレミスのスケールアウト バックアップ リポジトリの一部であった S3 オブジェクトからバックアップをインポートするには、次の手順を実行します。

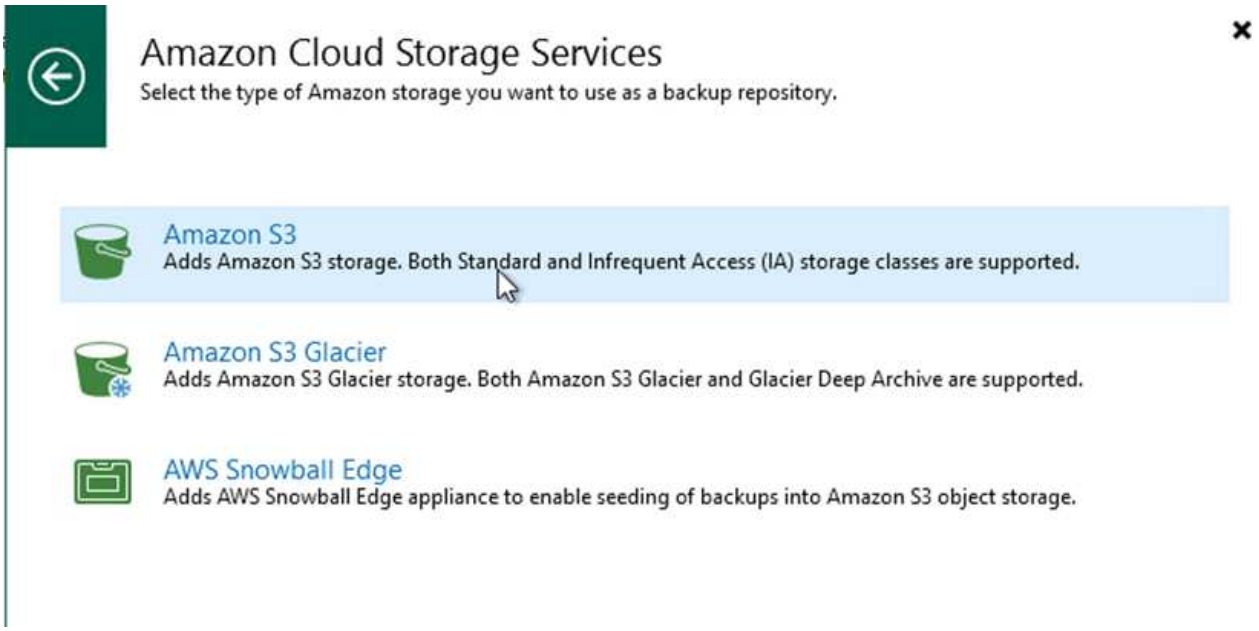
1. [バックアップ リポジトリ] に移動し、上部のメニューで [リポジトリの追加] をクリックして、[バックアップ リポジトリの追加] ウィザードを起動します。ウィザードの最初のページで、バックアップ リポジトリの種類としてオブジェクト ストレージを選択します。



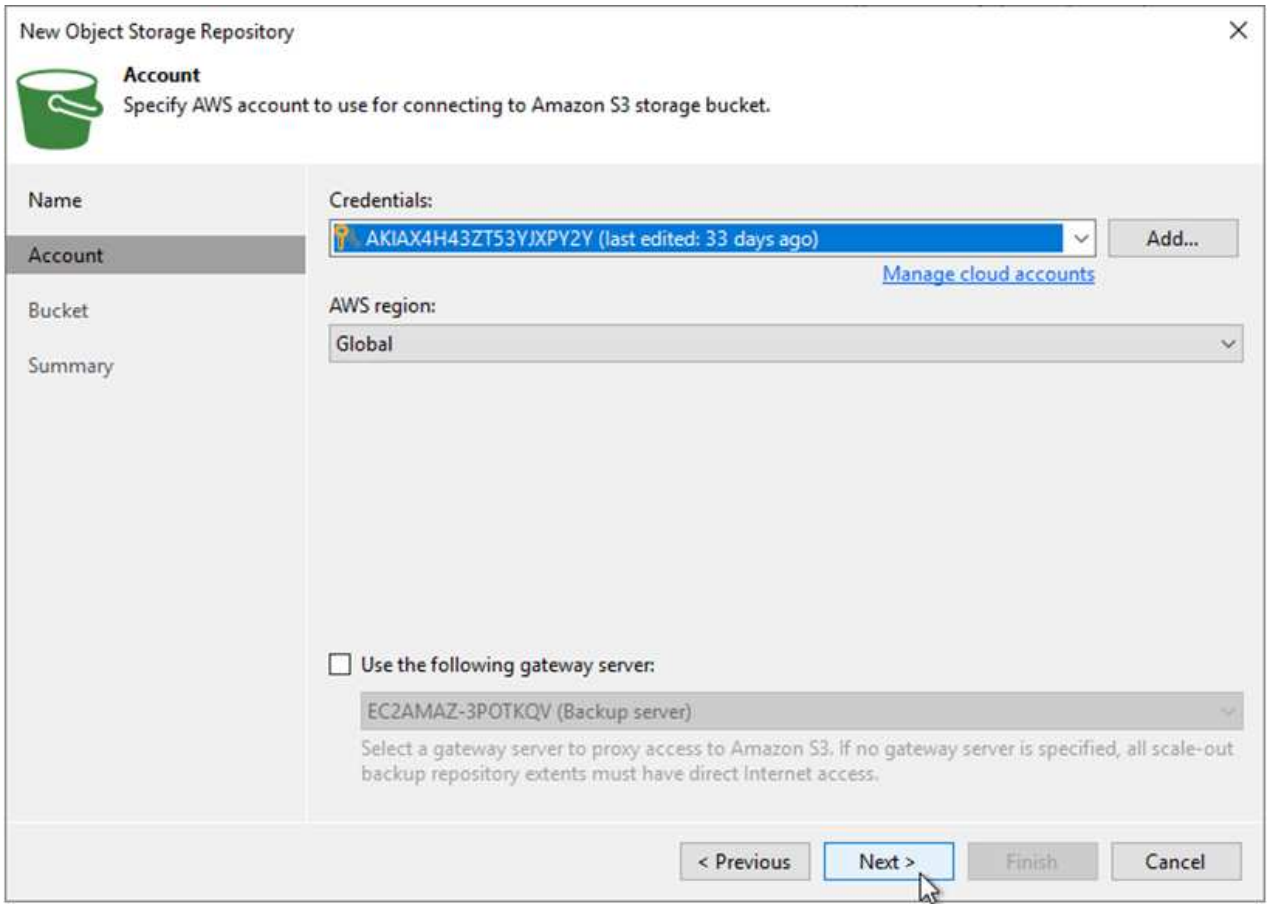
2. オブジェクトストレージタイプとして Amazon S3 を選択します。



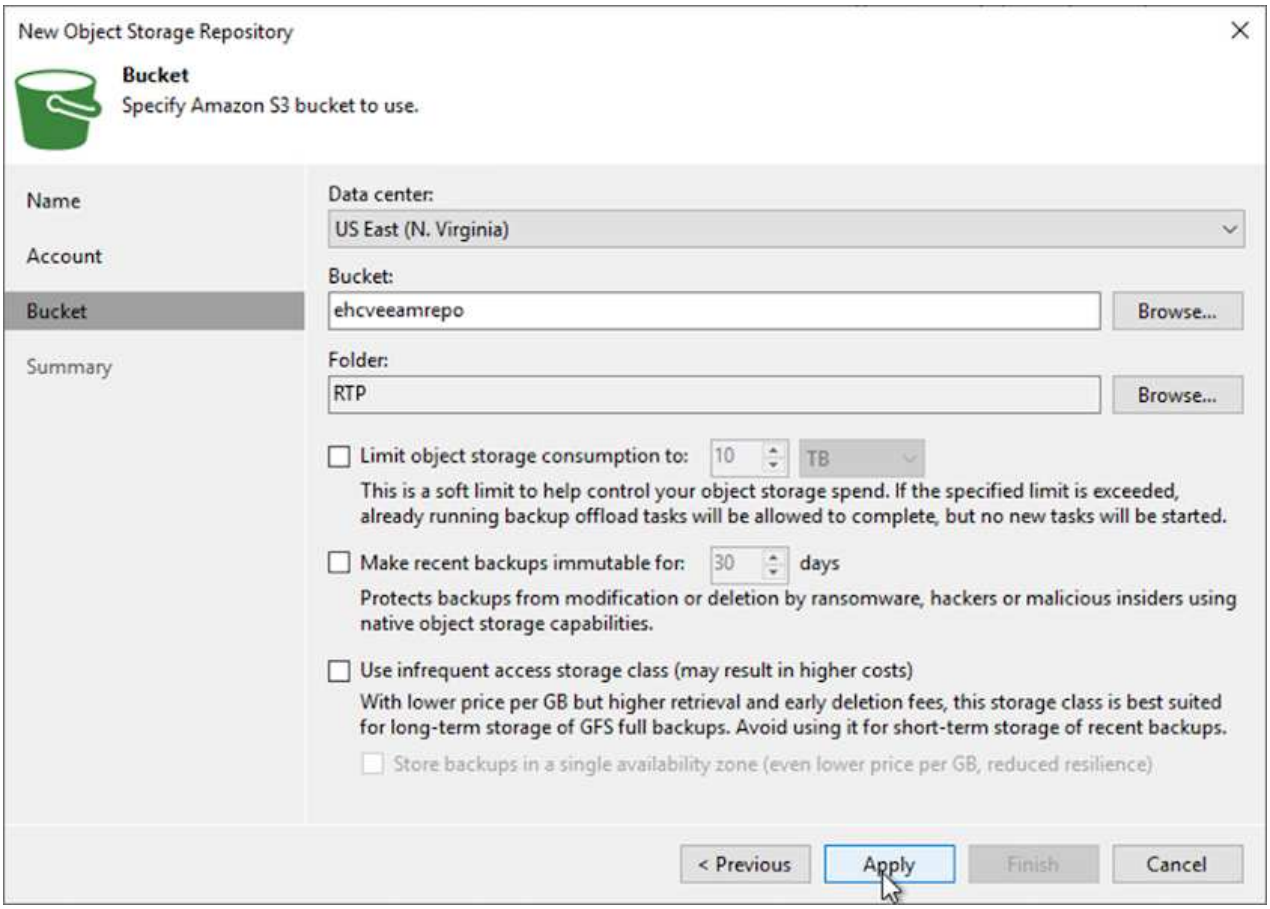
3. Amazon クラウド ストレージ サービスのリストから、Amazon S3 を選択します。



4. ドロップダウン リストから事前に入力した資格情報を選択するか、クラウド ストレージ リソースにアクセスするための新しい資格情報を追加します。 「次へ」をクリックして続行します。



5. バケット ページで、データ センター、バケット、フォルダー、および必要なオプションを入力します。[Apply]をクリックします。

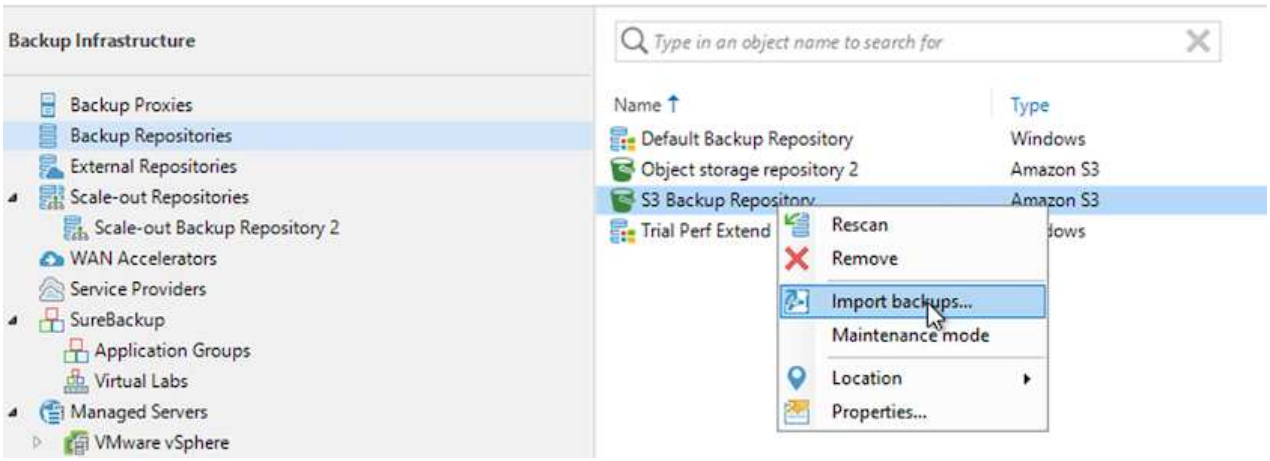


6. 最後に、「完了」を選択してプロセスを完了し、リポジトリを追加します。

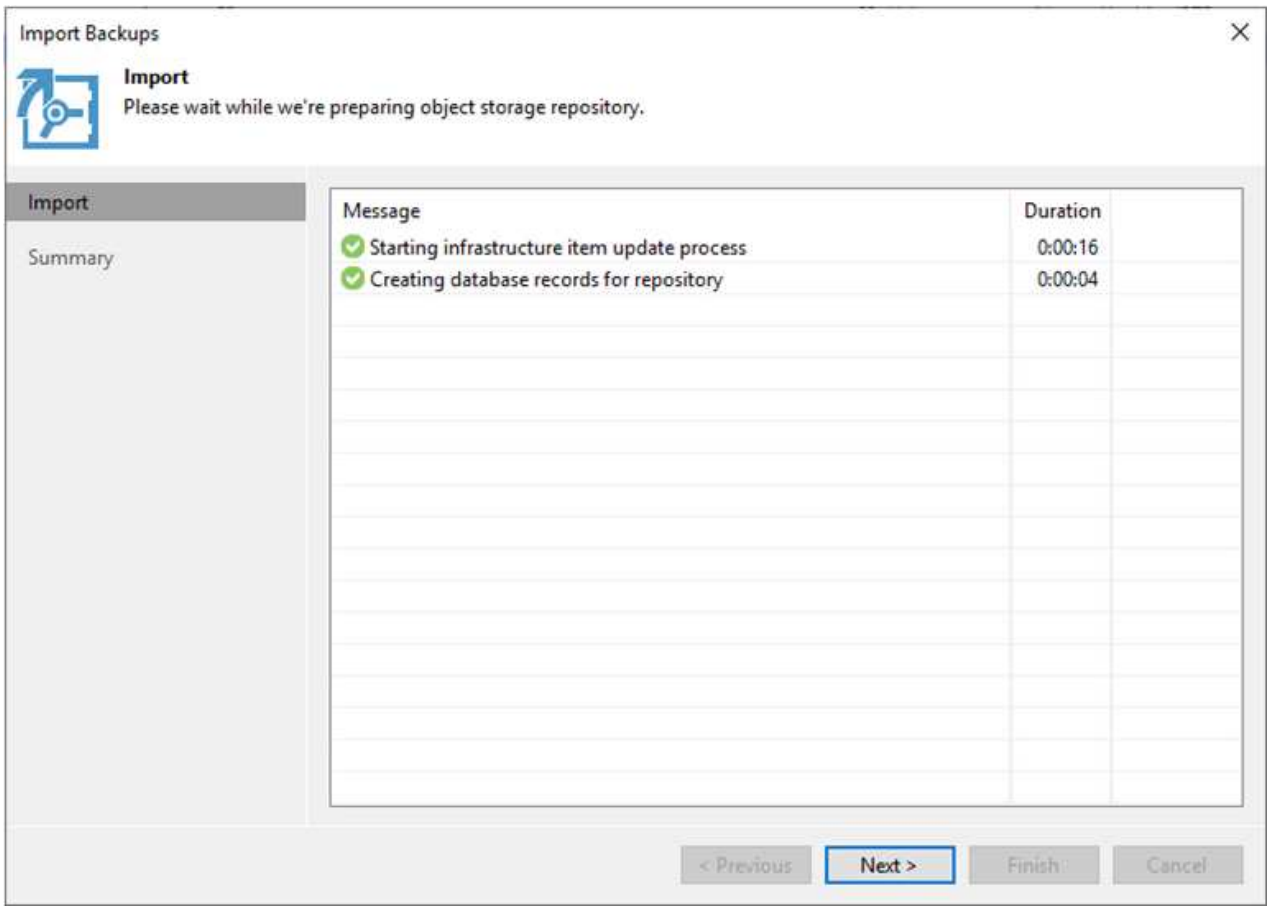
S3 オブジェクトストレージからバックアップをインポートする

前のセクションで追加した S3 リポジトリからバックアップをインポートするには、次の手順を実行します。

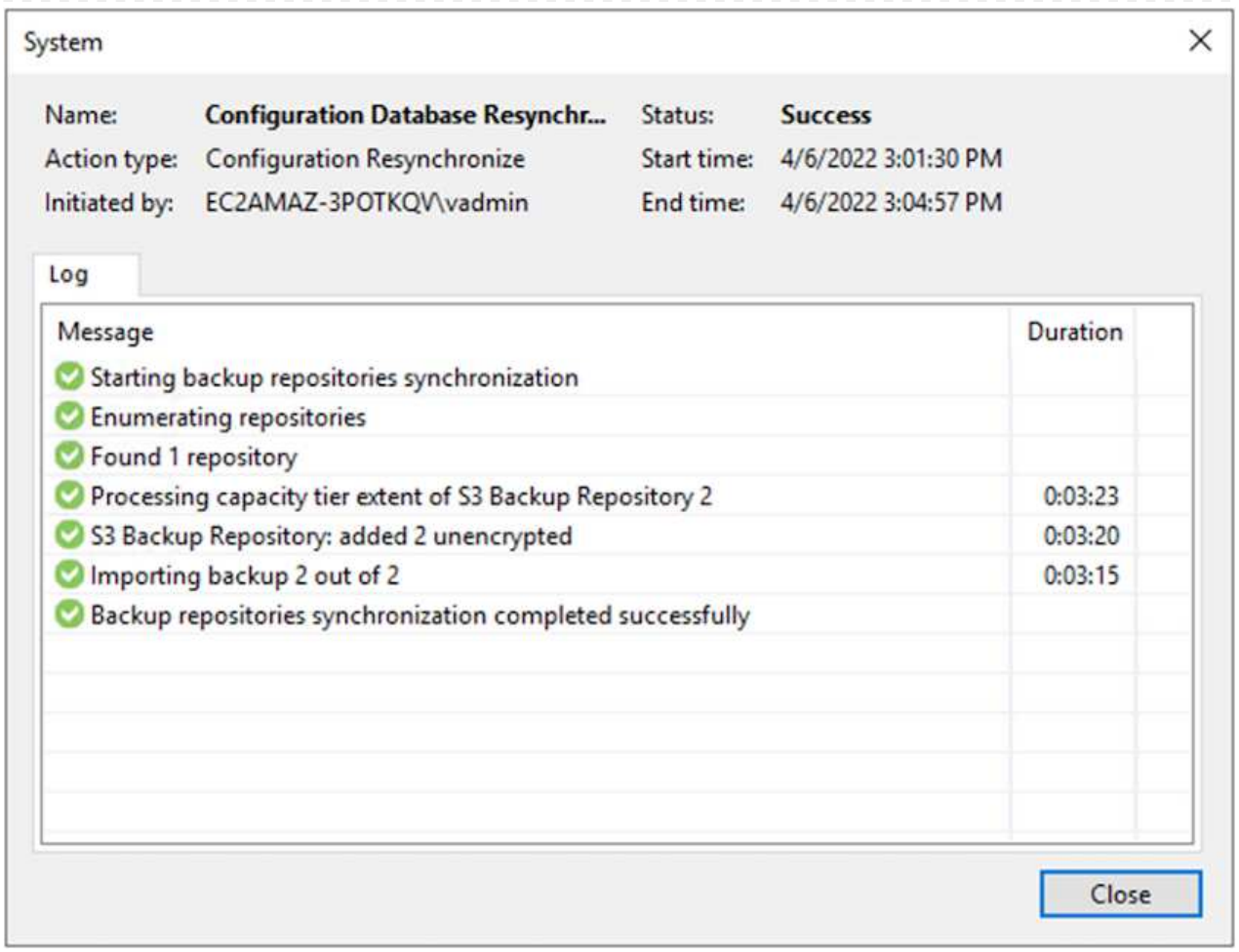
1. S3 バックアップ リポジトリから、[バックアップのインポート] を選択して、[バックアップのインポート] ウィザードを起動します。



2. インポート用のデータベース レコードが作成されたら、概要画面で [次へ] を選択し、[完了] を選択してインポート プロセスを開始します。

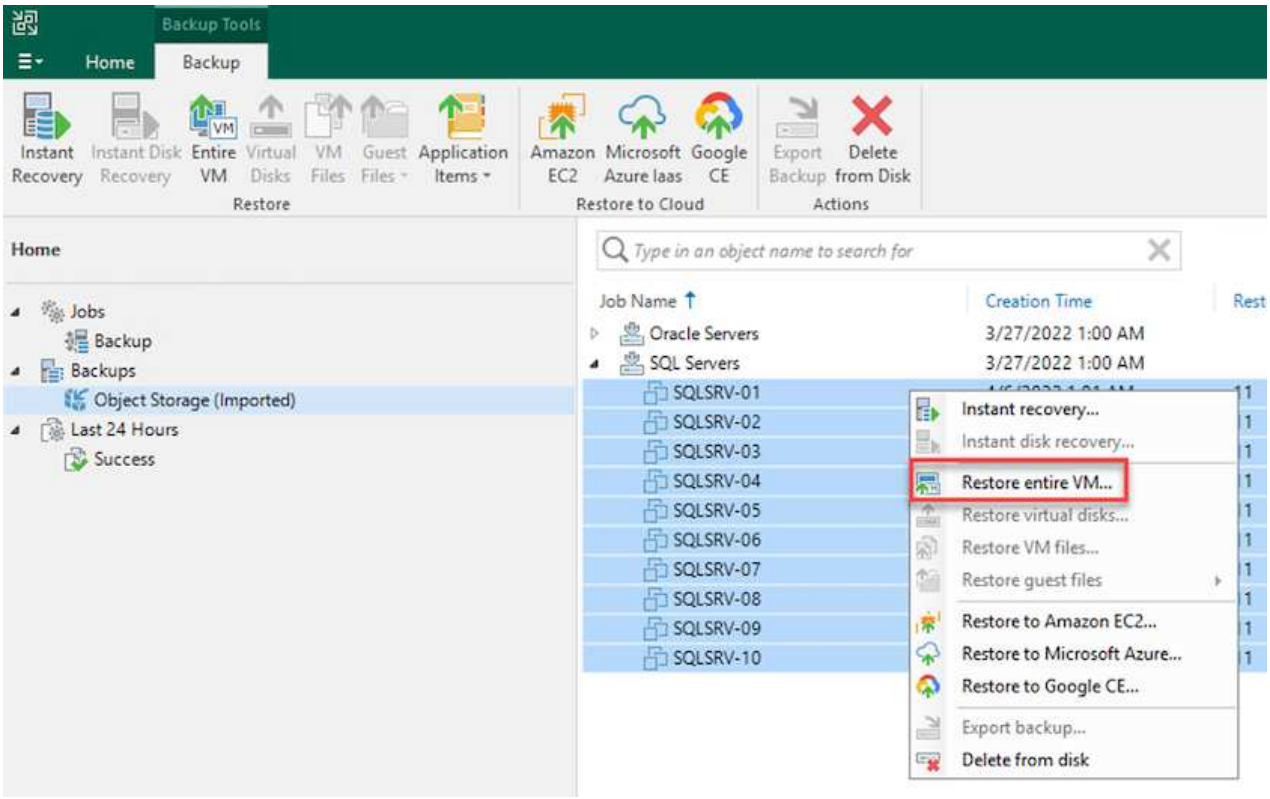


3. インポートが完了したら、VM を VMware Cloud クラスターに復元できます。

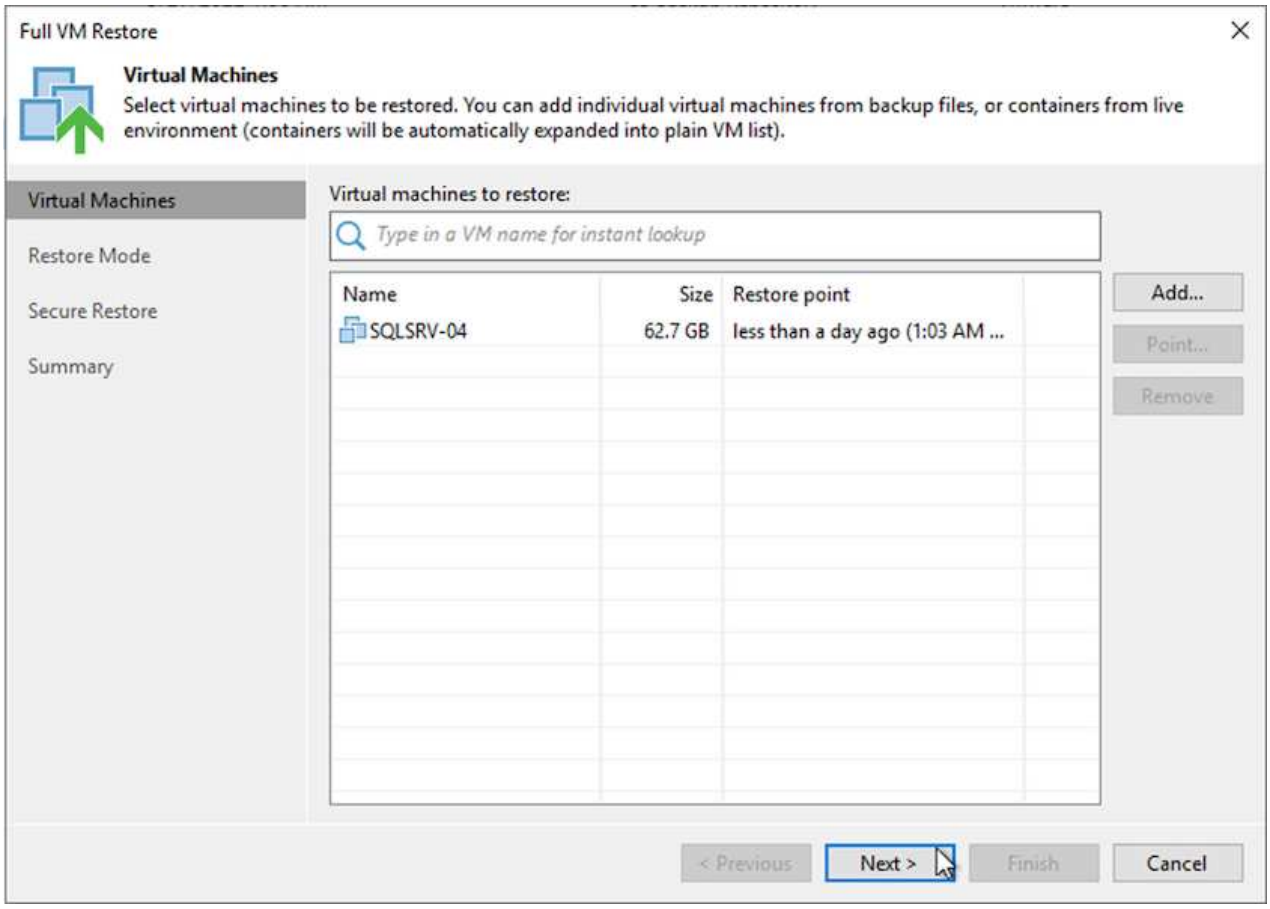

System
Name: Configuration Database Resynchr...
Status: Success
Action type: Configuration Resynchronize
Start time: 4/6/2022 3:01:30 PM
Initiated by: EC2AMAZ-3POTKQV\vadmin
End time: 4/6/2022 3:04:57 PM
Log
Message
Duration
Starting backup repositories synchronization
Enumerating repositories
Found 1 repository
Processing capacity tier extent of S3 Backup Repository 2
0:03:23
S3 Backup Repository: added 2 unencrypted
0:03:20
Importing backup 2 out of 2
0:03:15
Backup repositories synchronization completed successfully
Close

SQL および Oracle 仮想マシンを VMware Cloud on AWS ワークロード ドメイン/クラスタに復元するには、次の手順を実行します。

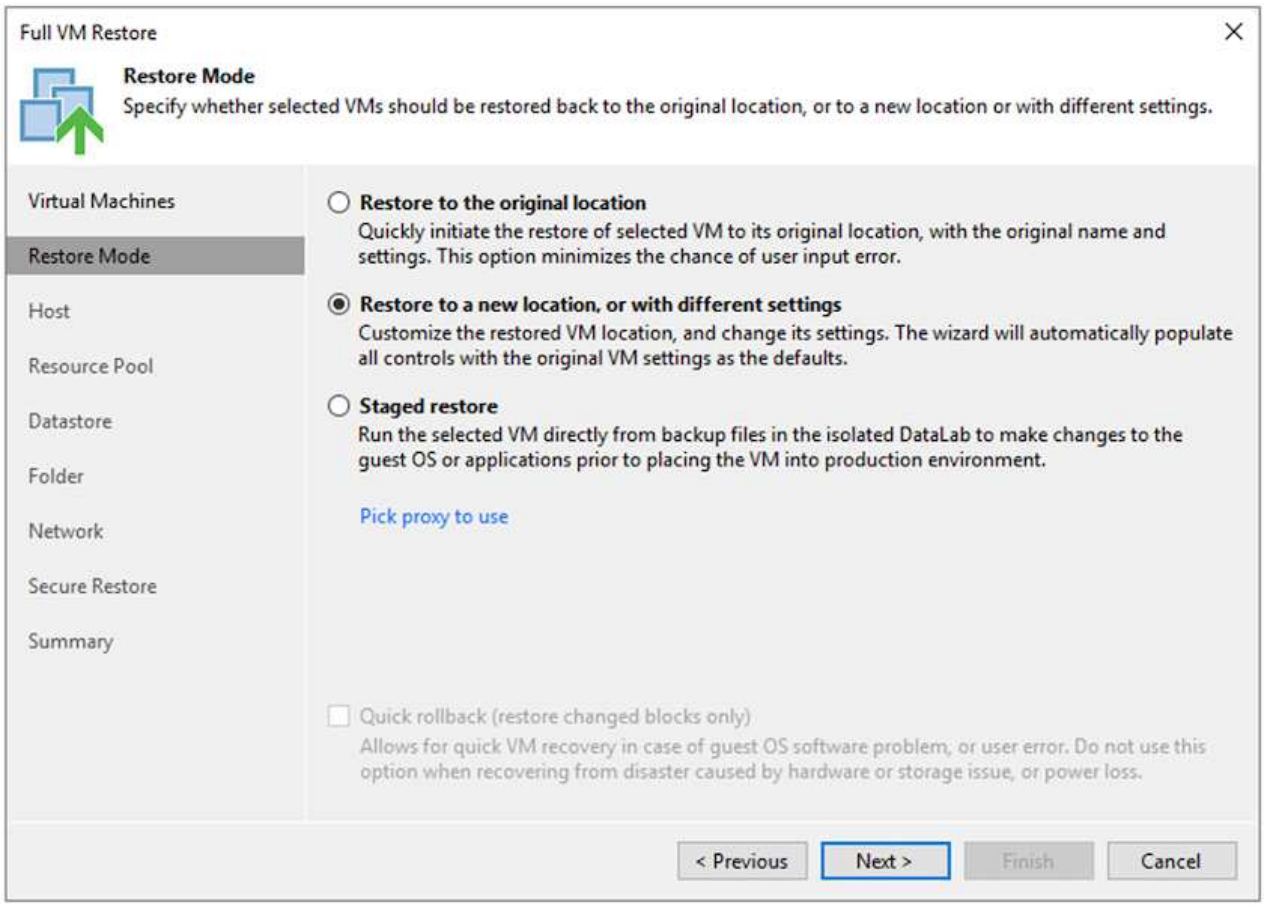
1. Veeam ホーム ページで、インポートされたバックアップを含むオブジェクト ストレージを選択し、復元する VM を選択して、右クリックし、[VM 全体の復元] を選択します。



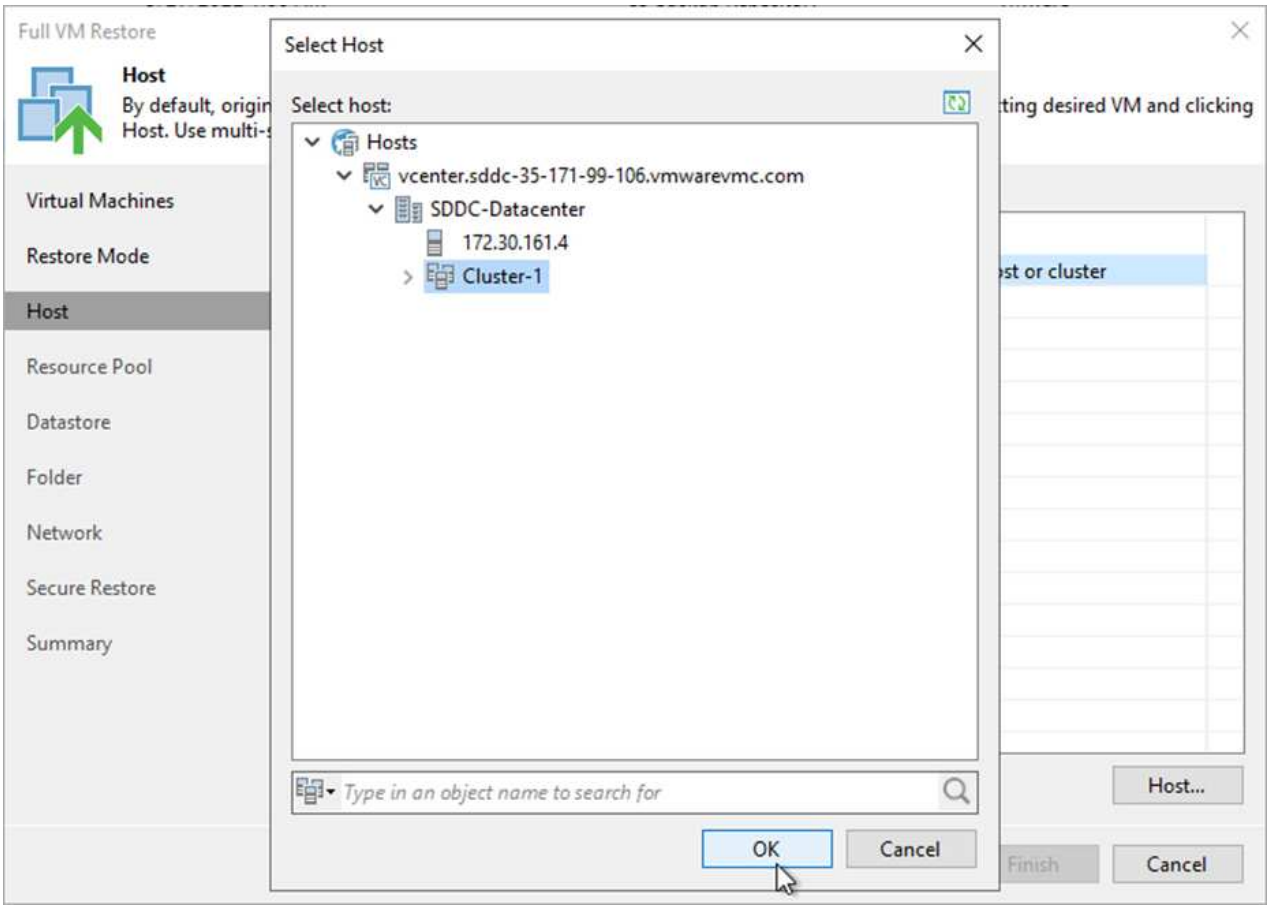
2. 完全な VM の復元ウィザードの最初のページで、必要に応じてバックアップする VM を変更し、[次へ] を選択します。



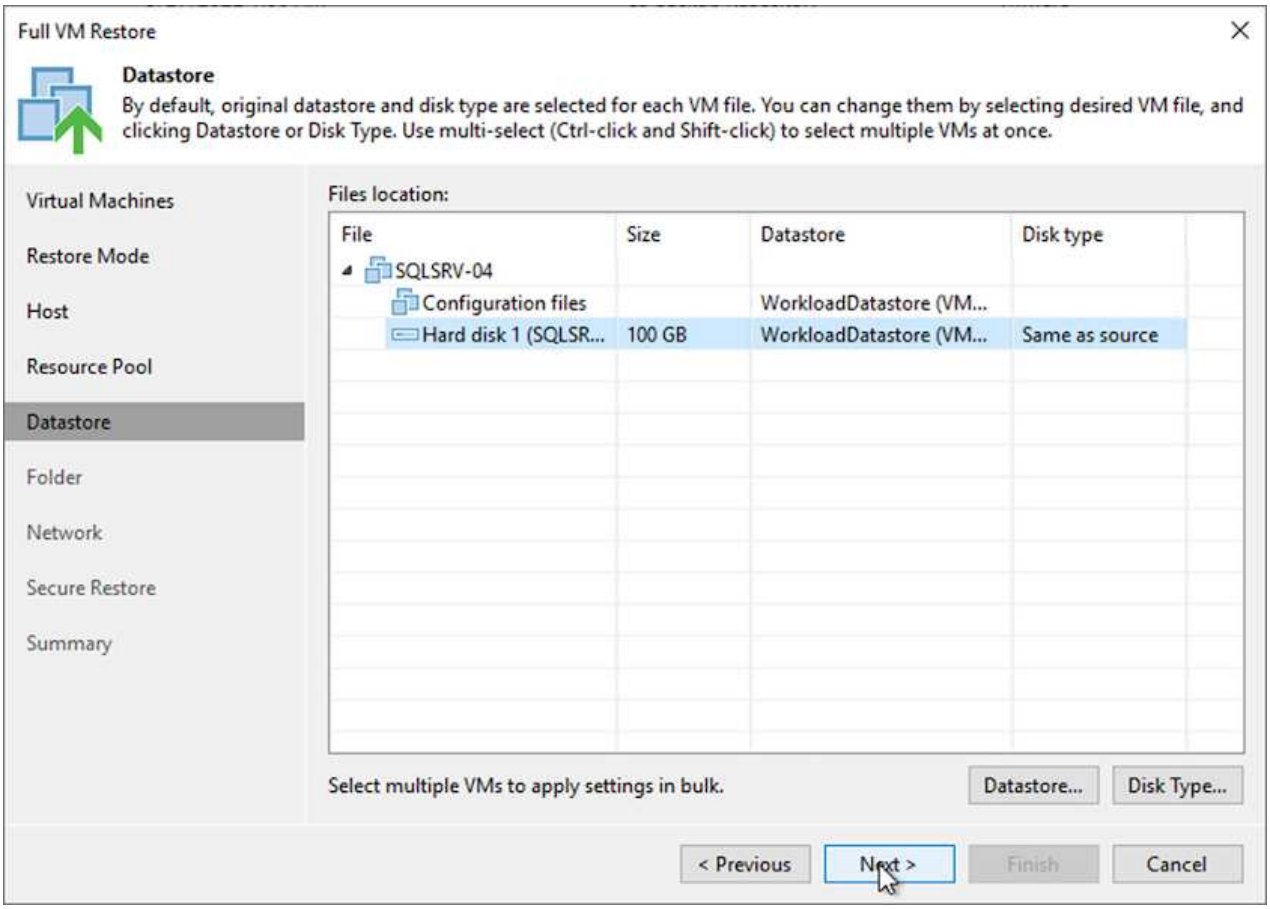
3. [復元モード] ページで、[新しい場所に復元] または [異なる設定で復元] を選択します。



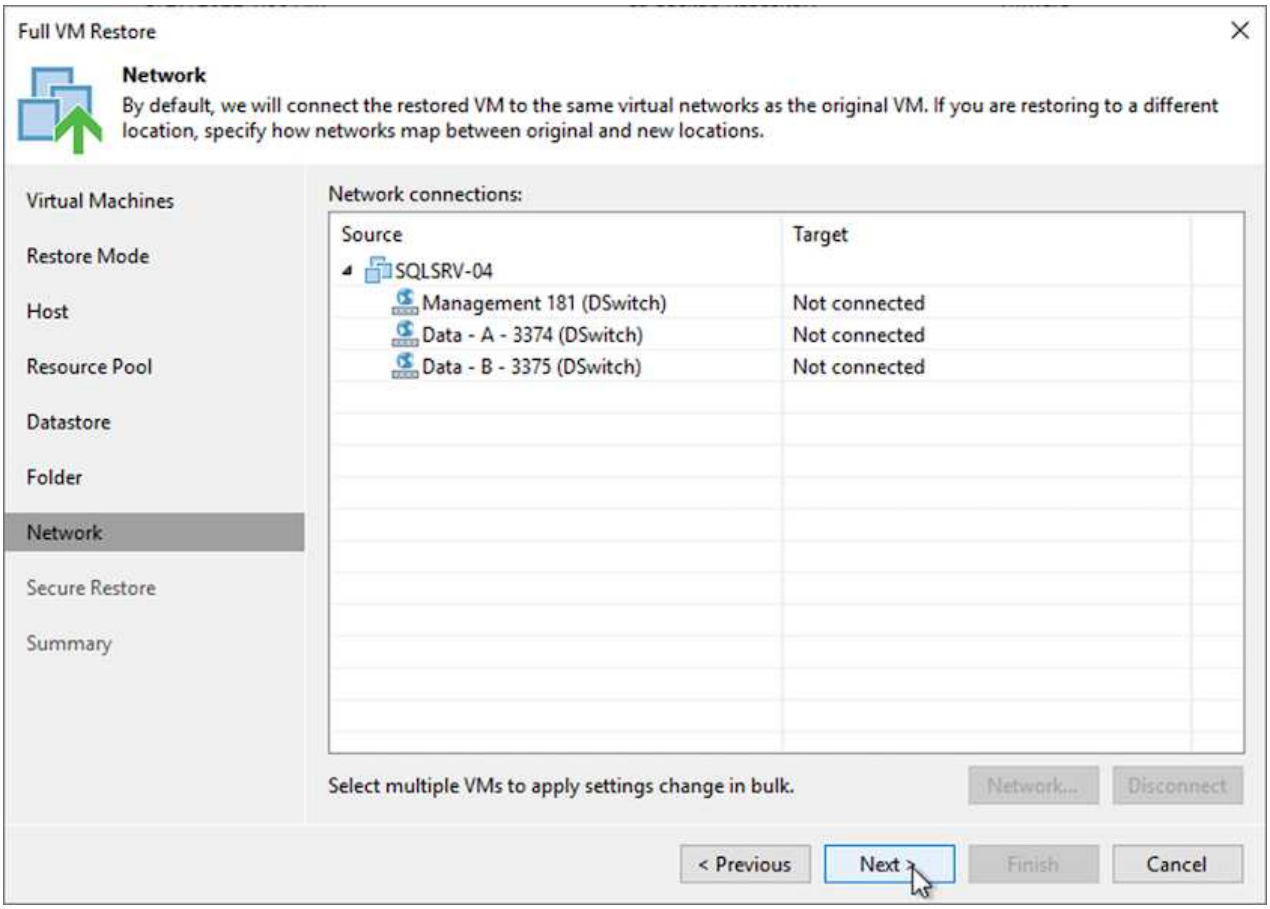
4. ホスト ページで、VM を復元するターゲット ESXi ホストまたはクラスターを選択します。

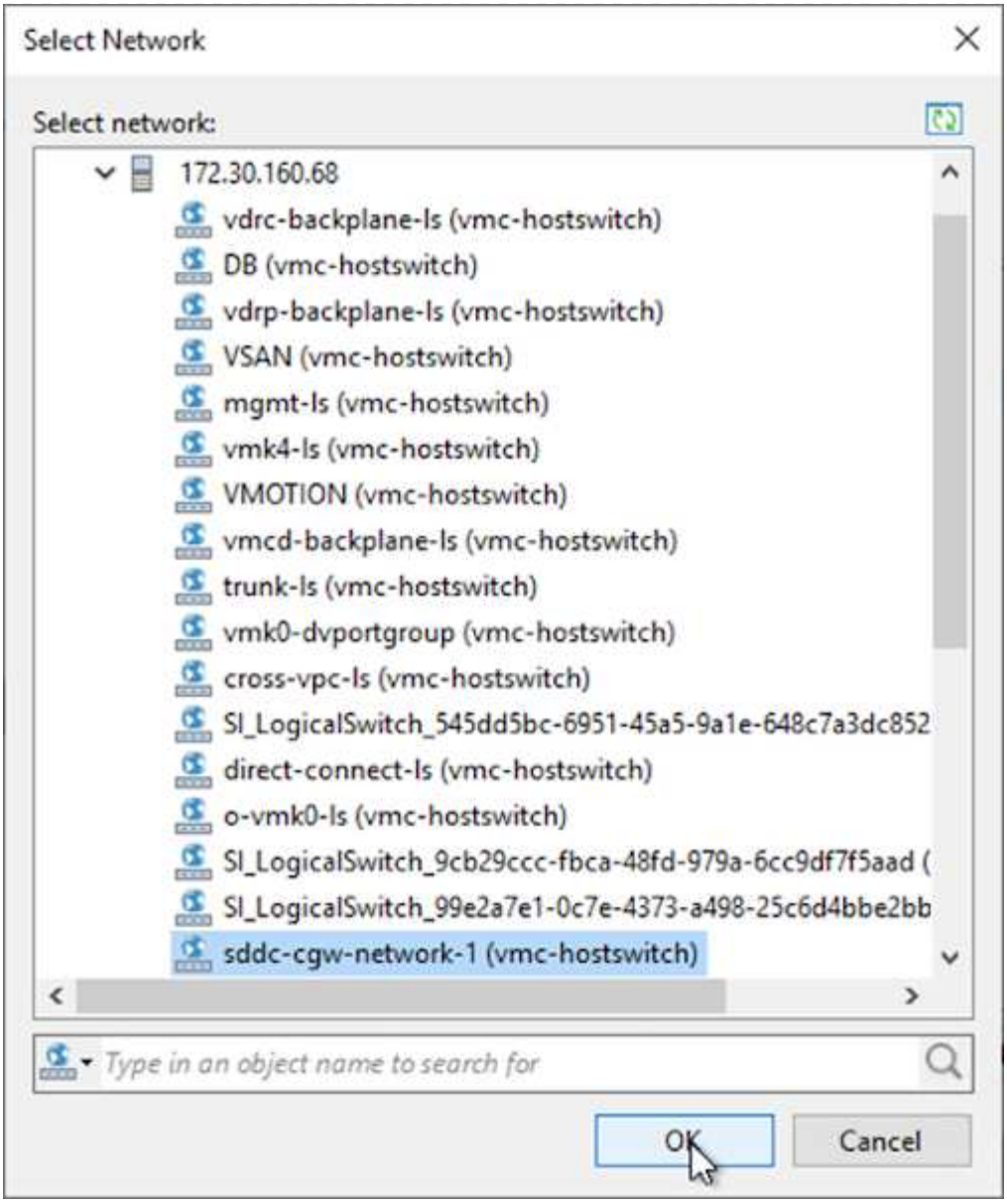


5. [データストア] ページで、構成ファイルとハード ディスクの両方のターゲット データストアの場所を選択します。



6. [ネットワーク] ページで、VM 上の元のネットワークを新しいターゲットの場所のネットワークにマップします。


Full VM Restore
Network
By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.
Virtual Machines
Restore Mode
Host
Resource Pool
Datastore
Folder
Network
Secure Restore
Summary
Network connections:
Source
Target
SQLSRV-04
Management 181 (DSwitch)
Not connected
Data - A - 3374 (DSwitch)
Not connected
Data - B - 3375 (DSwitch)
Not connected
Select multiple VMs to apply settings change in bulk.
Network...
Disconnect
< Previous
Next >
Finish
Cancel



7. 復元された VM をマルウェアスキャンするかどうかを選択し、概要ページを確認して、[完了] をクリックして復元を開始します。

SQL Server アプリケーション データを復元する

次のプロセスでは、オンプレミス サイトが動作不能になる災害が発生した場合に、AWS の VMware Cloud Services で SQL Server を復旧する方法について説明します。

回復手順を続行するには、次の前提条件が完了している必要があります。

1. Windows Server VM は、Veeam Full Restore を使用して VMware Cloud SDDC に復元されました。
2. セカンダリSnapCenterサーバーが確立され、 SnapCenterデータベースの復元と構成が、セクションに記載されている手順を使用して完了しました。"SnapCenter のバックアップおよび復元プロセスの概要。"

VM: SQL Server VM の復元後の構成

VM の復元が完了したら、 SnapCenter内でホスト VM を再検出する準備として、ネットワークなどの項目を構成する必要があります。

1. 管理および iSCSI または NFS に新しい IP アドレスを割り当てます。
2. ホストを Windows ドメインに参加させます。
3. ホスト名を DNS またはSnapCenterサーバー上のホスト ファイルに追加します。

SnapCenterプラグインが現在のドメインとは異なるドメイン資格情報を使用して展開された場合は、SQL Server VM 上の Windows 用プラグイン サービスのログオン アカウントを変更する必要があります。ログオン アカウントを変更した後、 SnapCenter SMCore 、Plug-in for Windows、および Plug-in for SQL Server サービスを再起動します。

SnapCenterで復元された VM を自動的に再検出するには、FQDN がオンプレミスのSnapCenterに最初に追加された VM と同一である必要があります。

SQL Server の復元用に **FSx** ストレージを構成する

SQL Server VM の災害復旧復元プロセスを実行するには、FSx クラスターから既存のSnapMirror関係を解除し、ボリュームへのアクセスを許可する必要があります。そのためには、次の手順を実行します。

1. SQL Server データベースとログ ボリュームの既存のSnapMirror関係を解除するには、FSx CLI から次のコマンドを実行します。

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

2. SQL Server Windows VM の iSCSI IQN を含むイニシエーター グループを作成して、LUN へのアクセスを許可します。

```
FSx-Dest::> igroup create -vserver DestSVM -igroup igroupName
-protocol iSCSI -ostype windows -initiator IQN
```

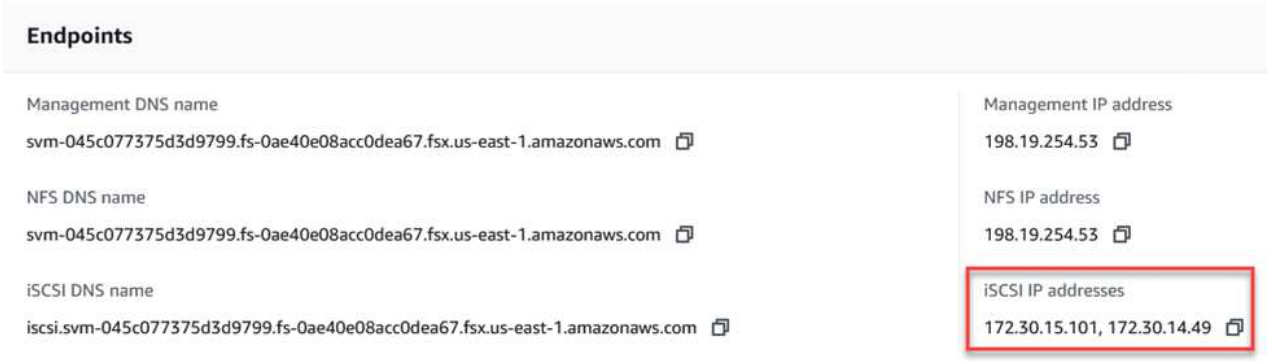
3. 最後に、作成したイニシエーター グループに LUN をマップします。

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup
igroupName
```

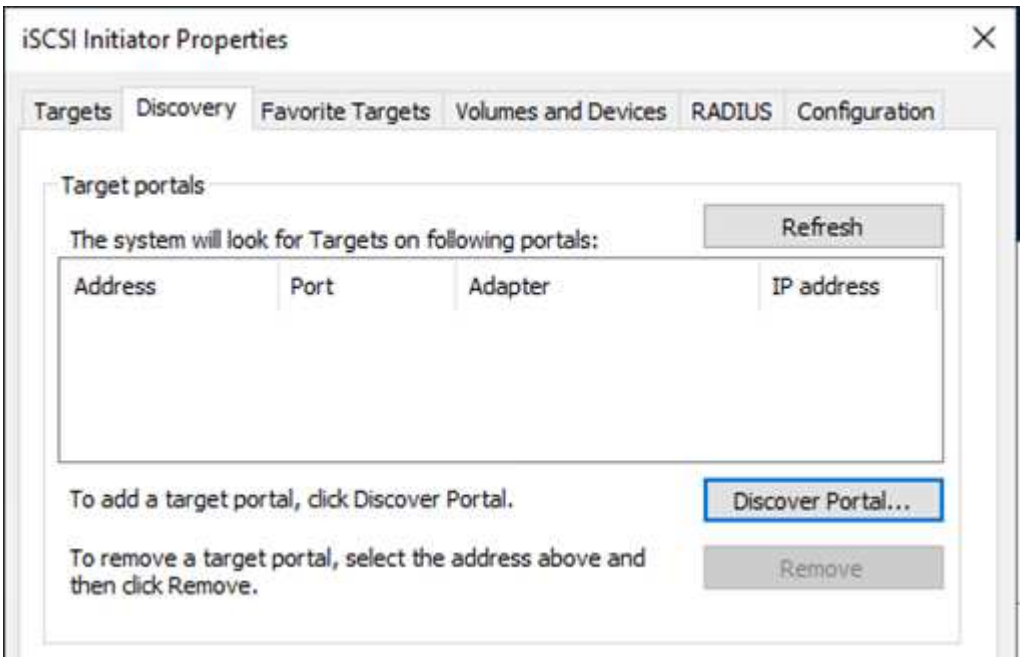
4. パス名を見つけるには、 `lun show`指示。

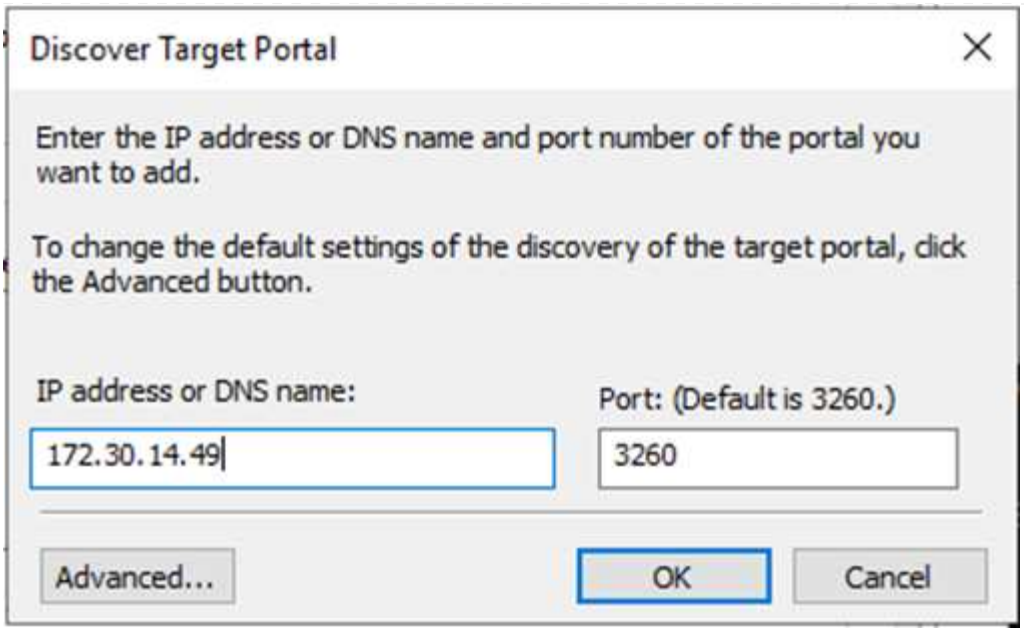
Windows VMをiSCSIアクセス用にセットアップし、ファイルシステムを検出する

1. SQL Server VM から、FSx インスタンス上の iSCSI ターゲット インターフェイスへの接続が確立された VMware ポート グループで通信するように iSCSI ネットワーク アダプターを設定します。
2. iSCSI イニシエーターのプロパティ ユーティリティを開き、[検出]、[お気に入りのターゲット]、および [ターゲット] タブの古い接続設定をクリアします。
3. FSx インスタンス/クラスター上の iSCSI 論理インターフェイスにアクセスするための IP アドレスを見つけます。これは、AWS コンソールのAmazon FSx > ONTAP > Storage Virtual Machines にあります。

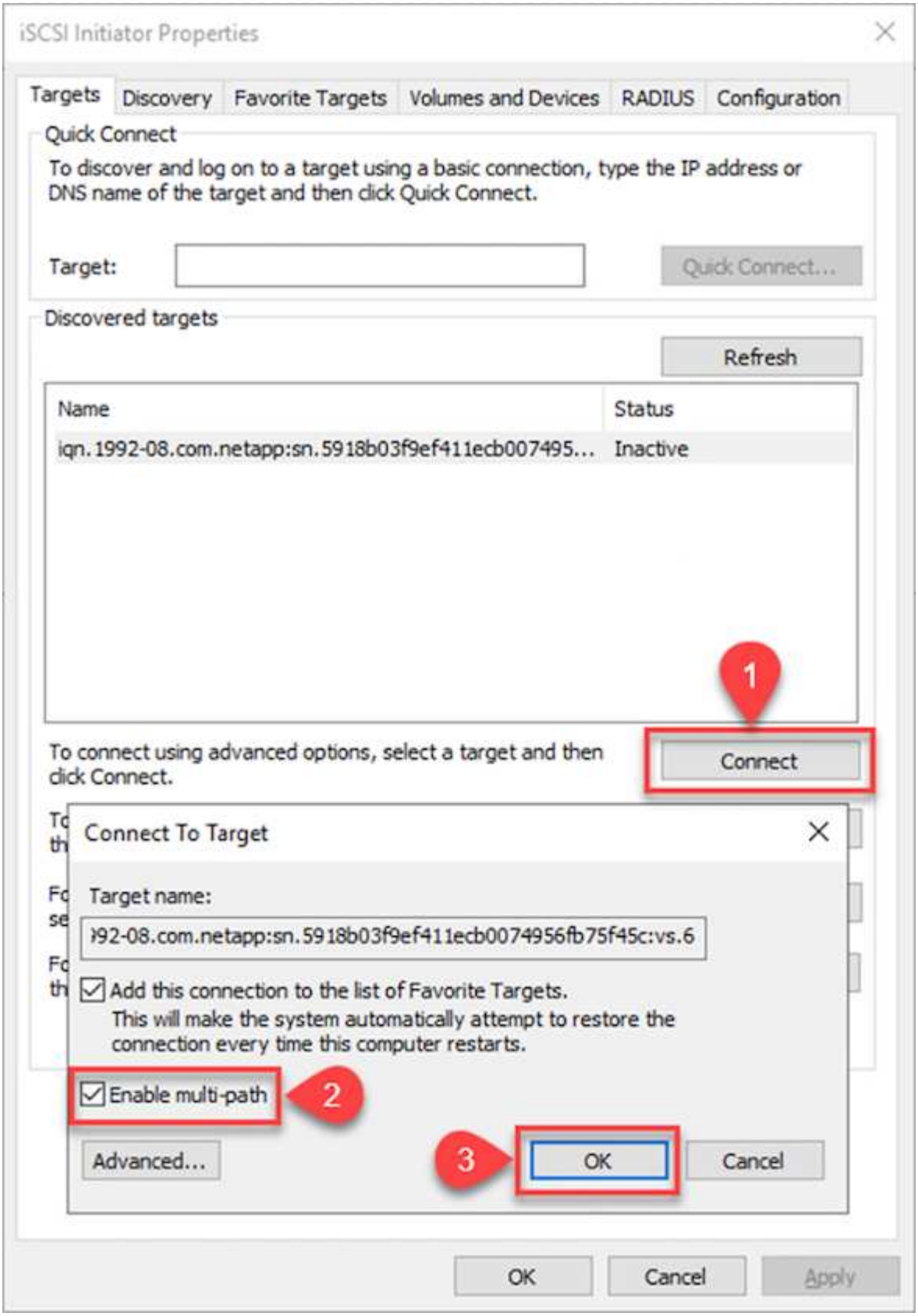


4. [検出] タブから [ポータルの検出] をクリックし、FSx iSCSI ターゲットの IP アドレスを入力します。

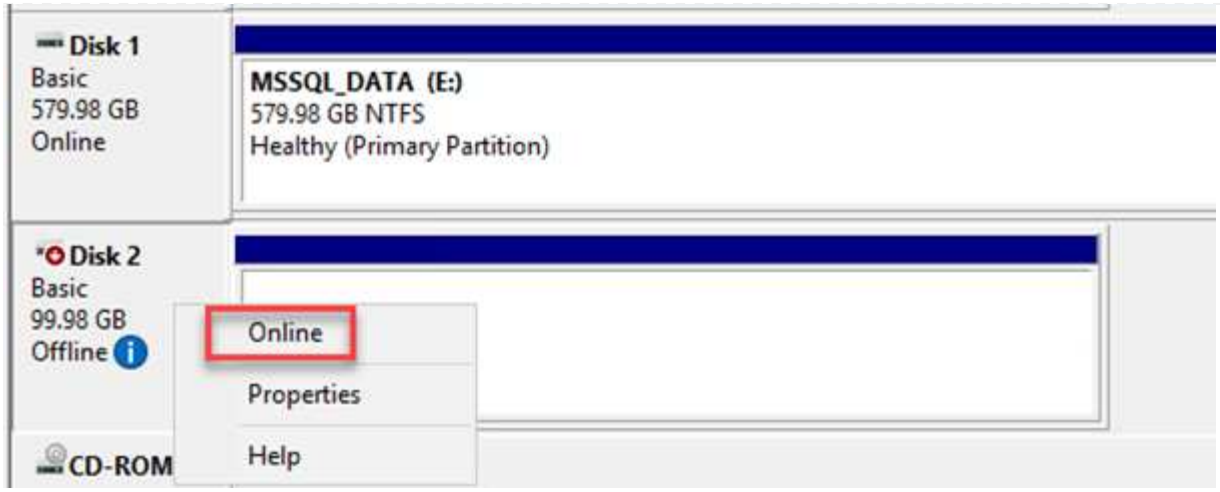




5. [ターゲット] タブで [接続] をクリックし、構成に応じて [マルチパスを有効にする] を選択してから [OK] をクリックし、ターゲットに接続します。

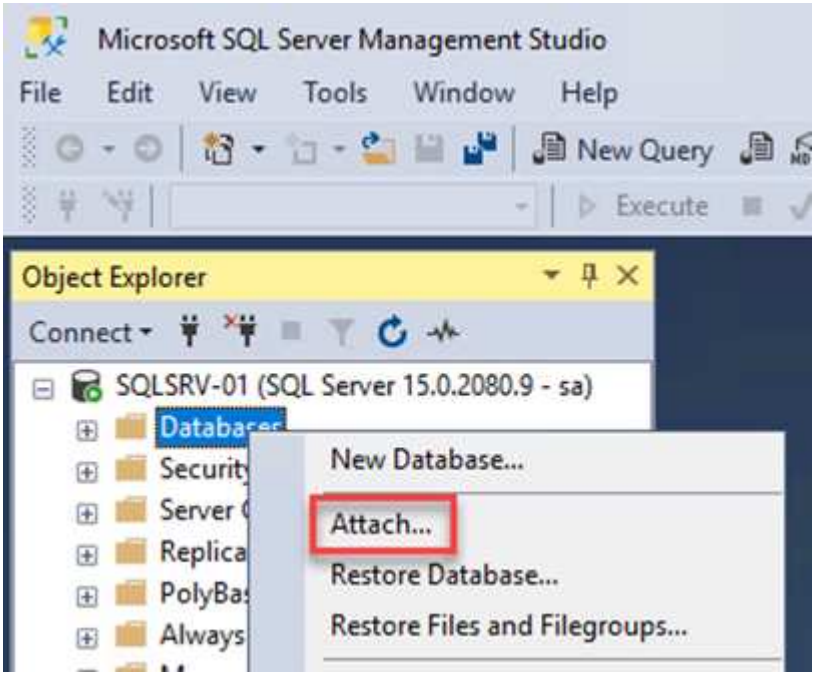


6. コンピュータの管理ユーティリティを開き、ディスクをオンラインにします。以前と同じドライブ文字が保持されていることを確認します。

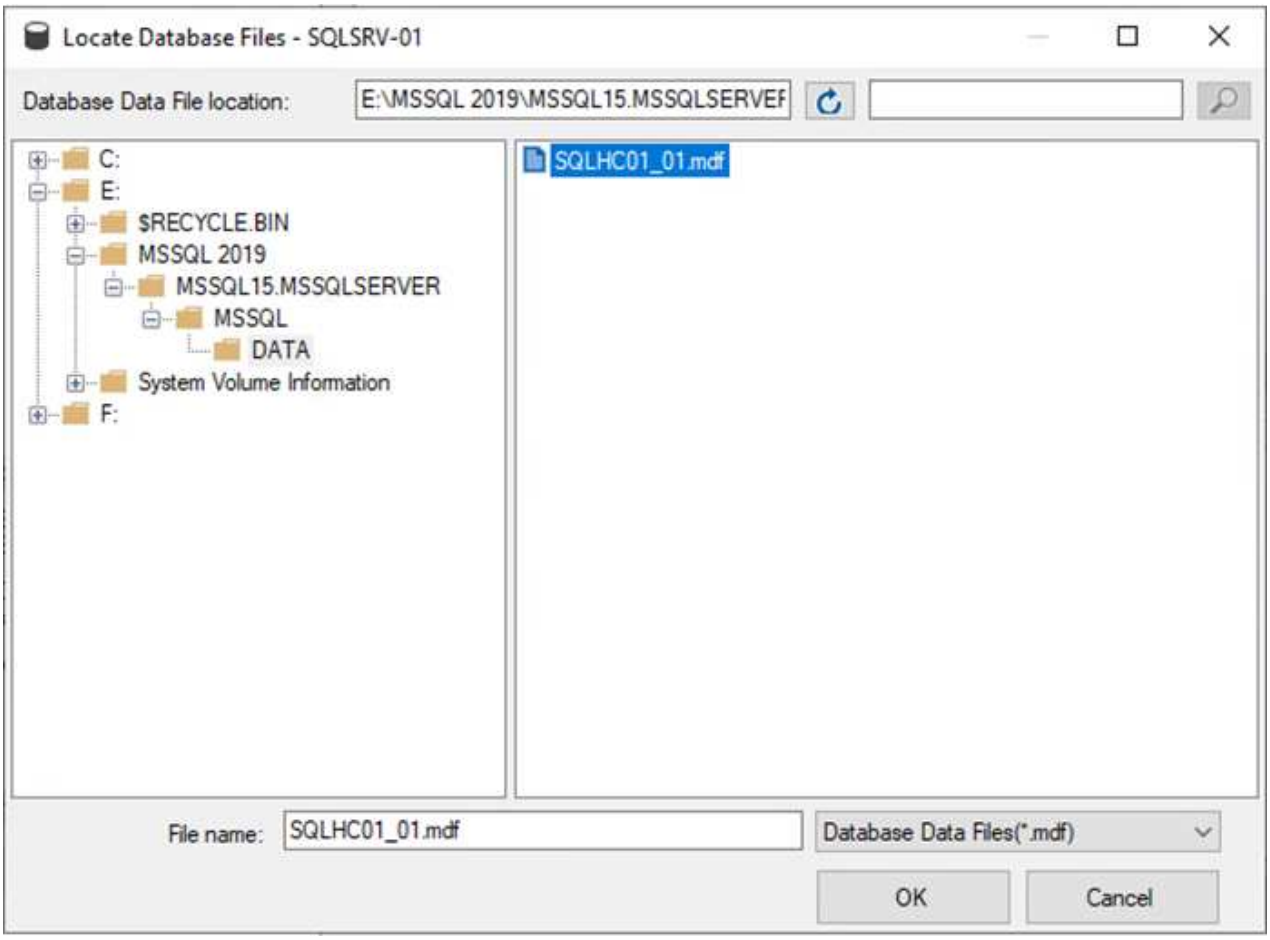

Disk 1
Basic
579.98 GB
Online
MSSQL_DATA (E:)
579.98 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
99.98 GB
Offline
Online
Properties
Help
CD-ROM

SQL Serverデータベースを接続する

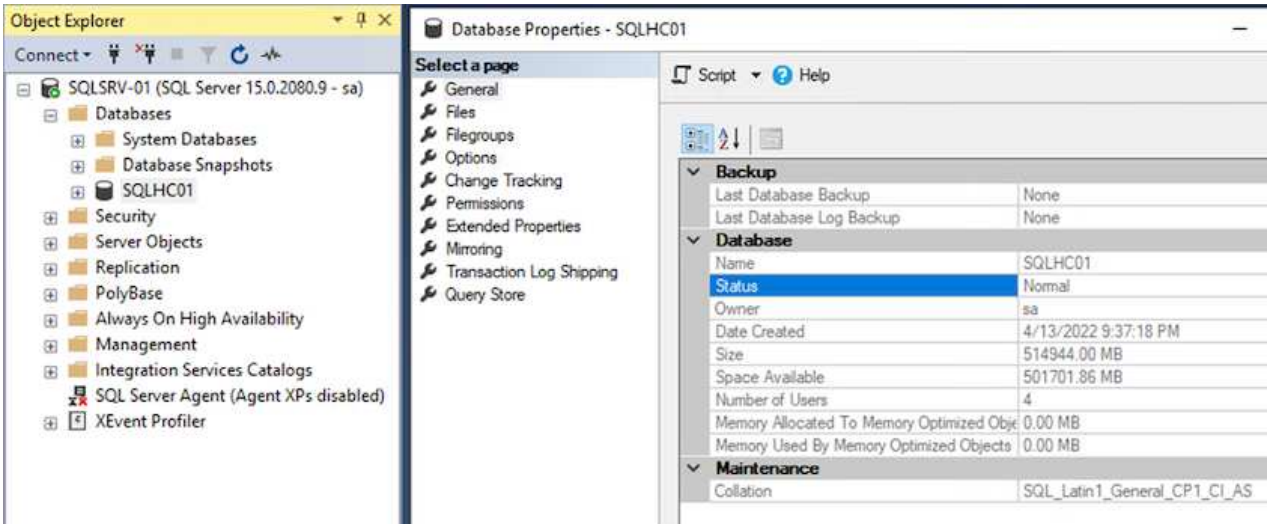
1. SQL Server VM から Microsoft SQL Server Management Studio を開き、[アタッチ] を選択してデータベースへの接続プロセスを開始します。



2. [追加] をクリックし、SQL Server プライマリ データベース ファイルが含まれているフォルダーに移動して選択し、[OK] をクリックします。



3. トランザクション ログが別のドライブにある場合は、トランザクション ログが含まれているフォルダーを選択します。
4. 完了したら、「OK」をクリックしてデータベースを接続します。

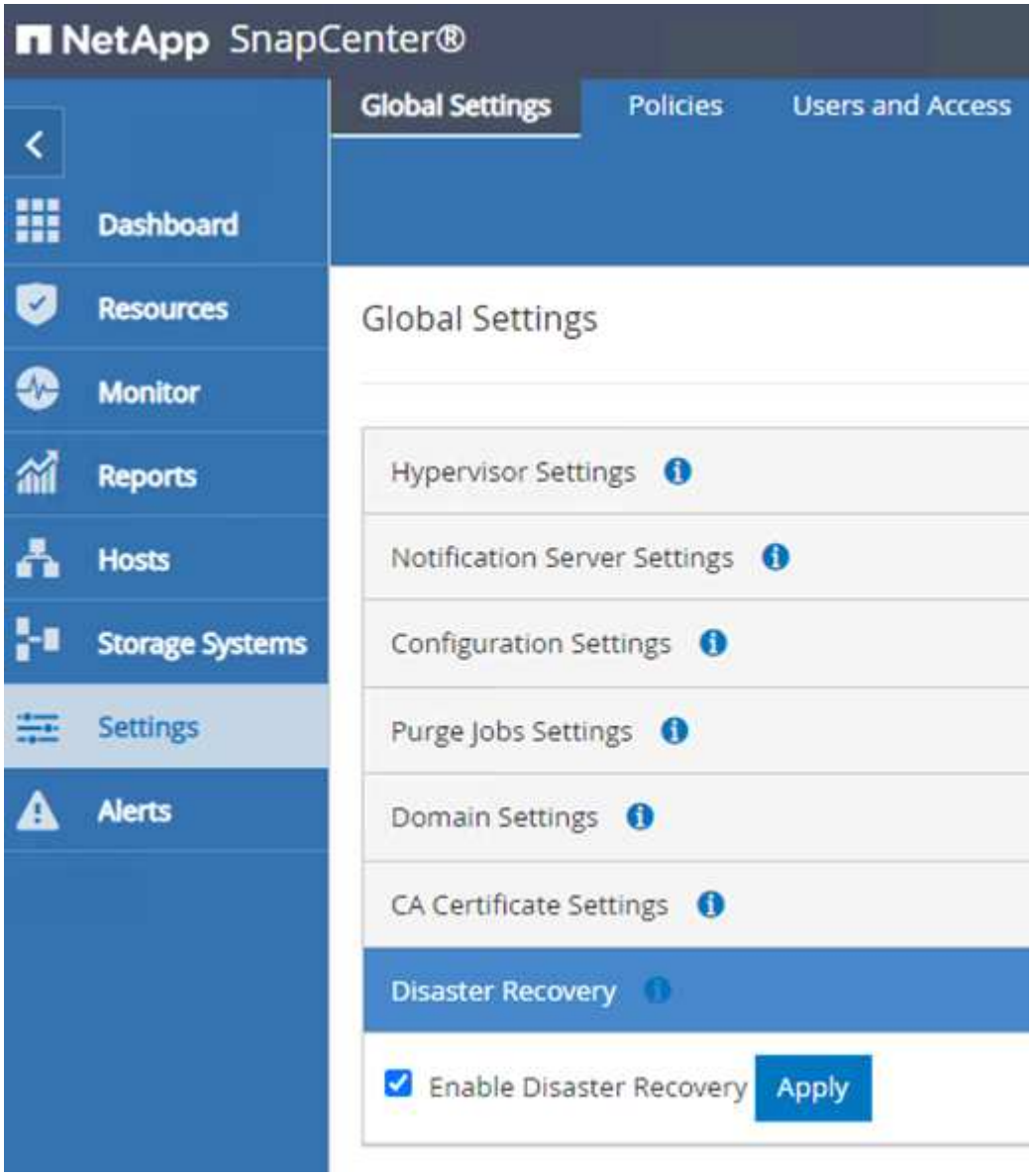


SnapCenterと SQL Server プラグインの通信を確認する

SnapCenterデータベースが以前の状態に復元されると、SQL Server ホストが自動的に再検出されます。これが正しく機能するには、次の前提条件に留意してください。

- SnapCenter を災害復旧モードにする必要があります。これは、Swagger API または災害復旧のグローバル設定を通じて実行できます。
- SQL Server の FQDN は、オンプレミスのデータセンターで実行されていたインスタンスと同一である必要があります。
- 元のSnapMirror関係を解除する必要があります。
- データベースを含む LUN は、SQL Server インスタンスにマウントされ、データベースが接続されている必要があります。

SnapCenterが災害復旧モードになっていることを確認するには、 SnapCenter Web クライアント内から [設定] に移動します。 [グローバル設定] タブに移動し、[災害復旧] をクリックします。 「災害復旧を有効にする」チェックボックスが有効になっていることを確認します。



Oracleアプリケーションデータの復元

次のプロセスでは、オンプレミス サイトが動作不能になる災害が発生した場合に、AWS の VMware Cloud Services で Oracle アプリケーション データを復旧する方法について説明します。

回復手順を続行するには、次の前提条件を完了してください。

1. Oracle Linux サーバー VM は、Veeam Full Restore を使用して VMware Cloud SDDC に復元されました。
2. セカンダリSnapCenterサーバーが確立され、このセクションで概説されている手順を使用してSnapCenterデータベースと構成ファイルが復元されました。"SnapCenter のバックアップおよび復元プロセスの概要。"

FSx for Oracle の復元を構成する **– SnapMirror**関係を解除する

FSx ONTAPインスタンスでホストされているセカンダリ ストレージ ボリュームを Oracle サーバーからアクセスできるようにするには、まず既存のSnapMirror関係を解除する必要があります。

1. FSx CLI にログインした後、次のコマンドを実行して、正しい名前でフィルタリングされたボリュームを表示します。

```
FSx-Dest::> volume show -volume VolumeName*
```

```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
ora_svm_dest
          oraclesrv_03_u01_dest
                       aggr1        online     DP        100GB    93.12GB    6%
ora_svm_dest
          oraclesrv_03_u02_dest
                       aggr1        online     DP        200GB    34.98GB   82%
ora_svm_dest
          oraclesrv_03_u03_dest
                       aggr1        online     DP        150GB    33.37GB   77%
3 entries were displayed.

FsxId0ae40e08acc0dea67::>
```

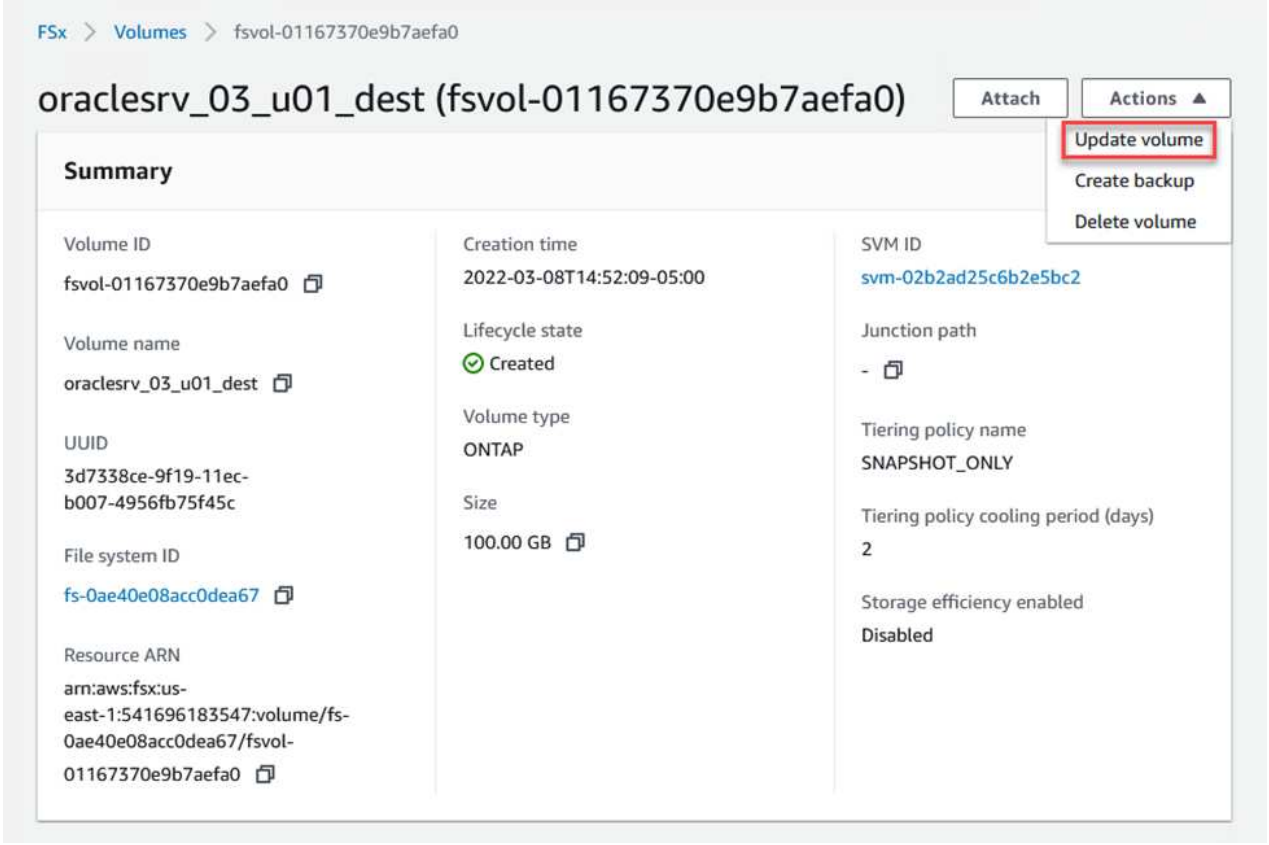
2. 既存のSnapMirror関係を解除するには、次のコマンドを実行します。

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

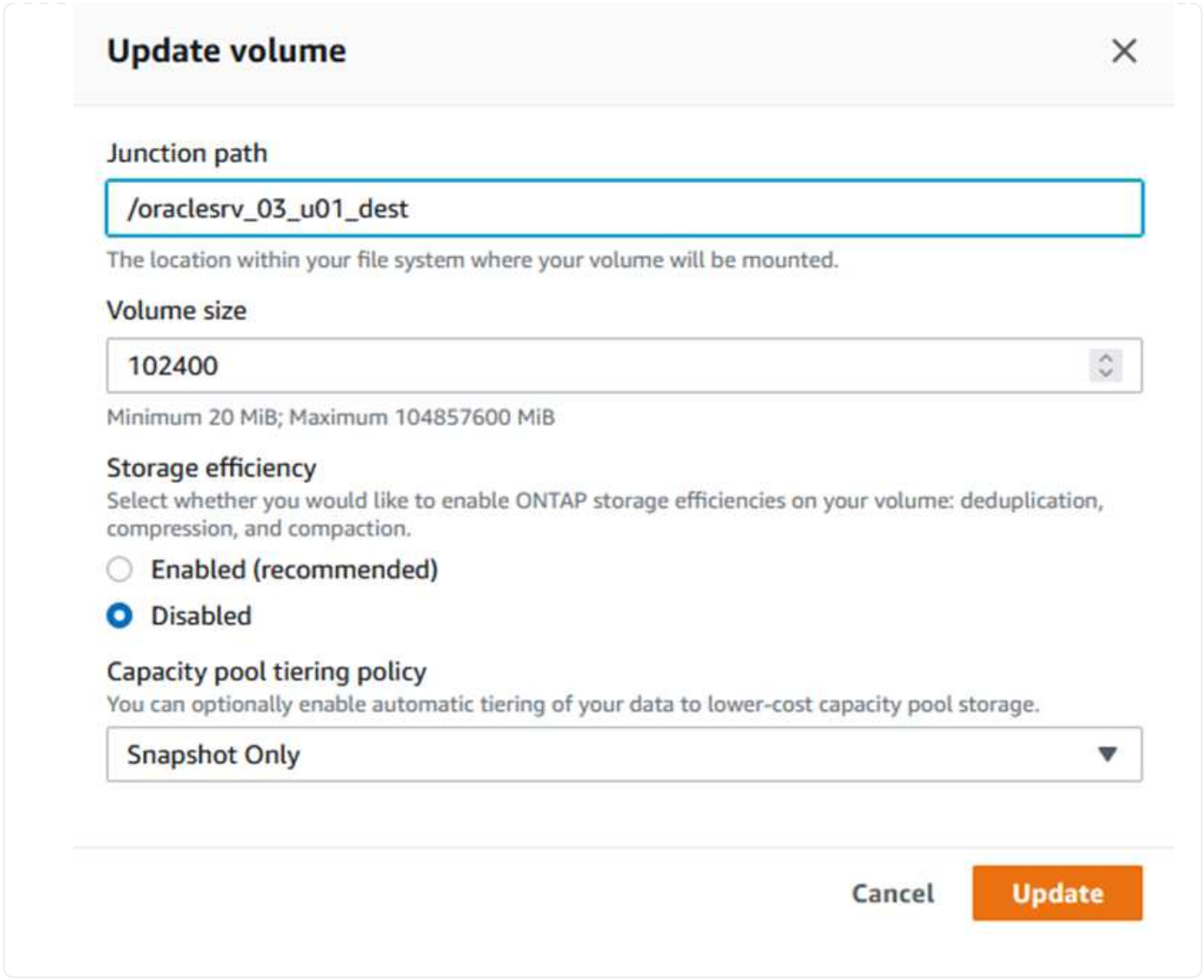
```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".
```

3. Amazon FSxウェブクライアントでジャンクションパスを更新します。



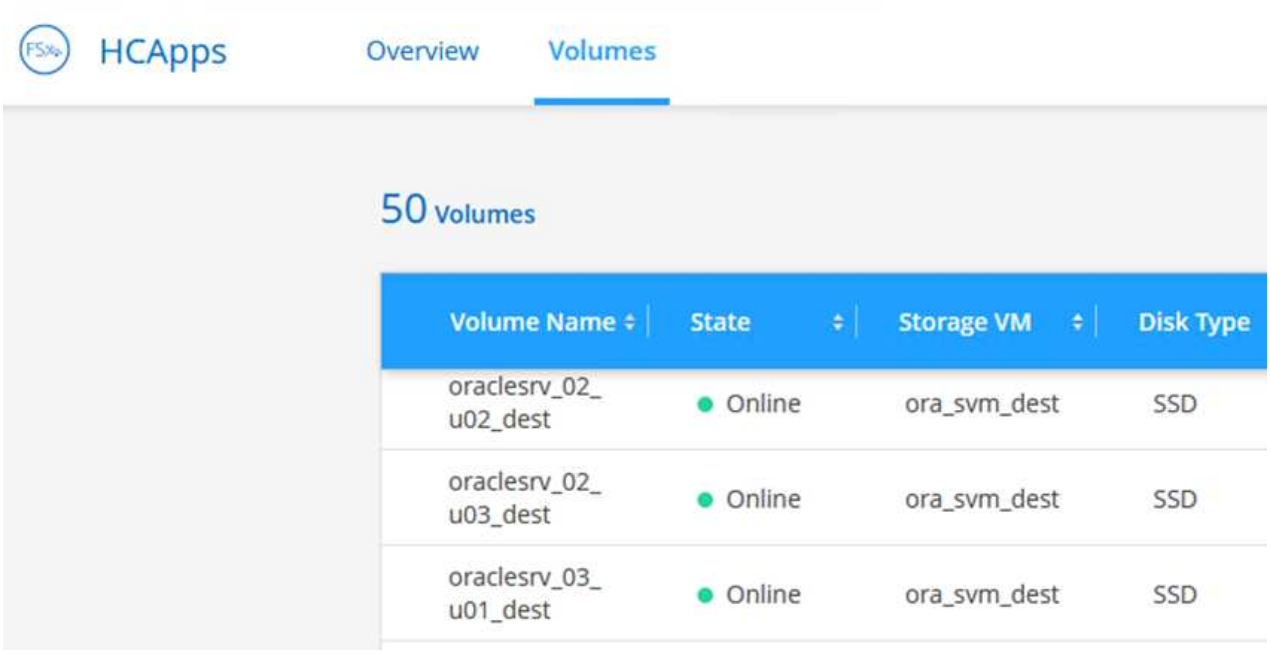
4. ジャンクション パス名を追加し、[更新] をクリックします。 Oracle サーバーから NFS ボリュームをマウントするときに、このジャンクション パスを指定します。


Update volume
Junction path
/oraclesrv_03_u01_dest
The location within your file system where your volume will be mounted.
Volume size
102400
Minimum 20 MiB; Maximum 104857600 MiB
Storage efficiency
Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.
Enabled (recommended)
Disabled
Capacity pool tiering policy
You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.
Snapshot Only
Cancel
Update

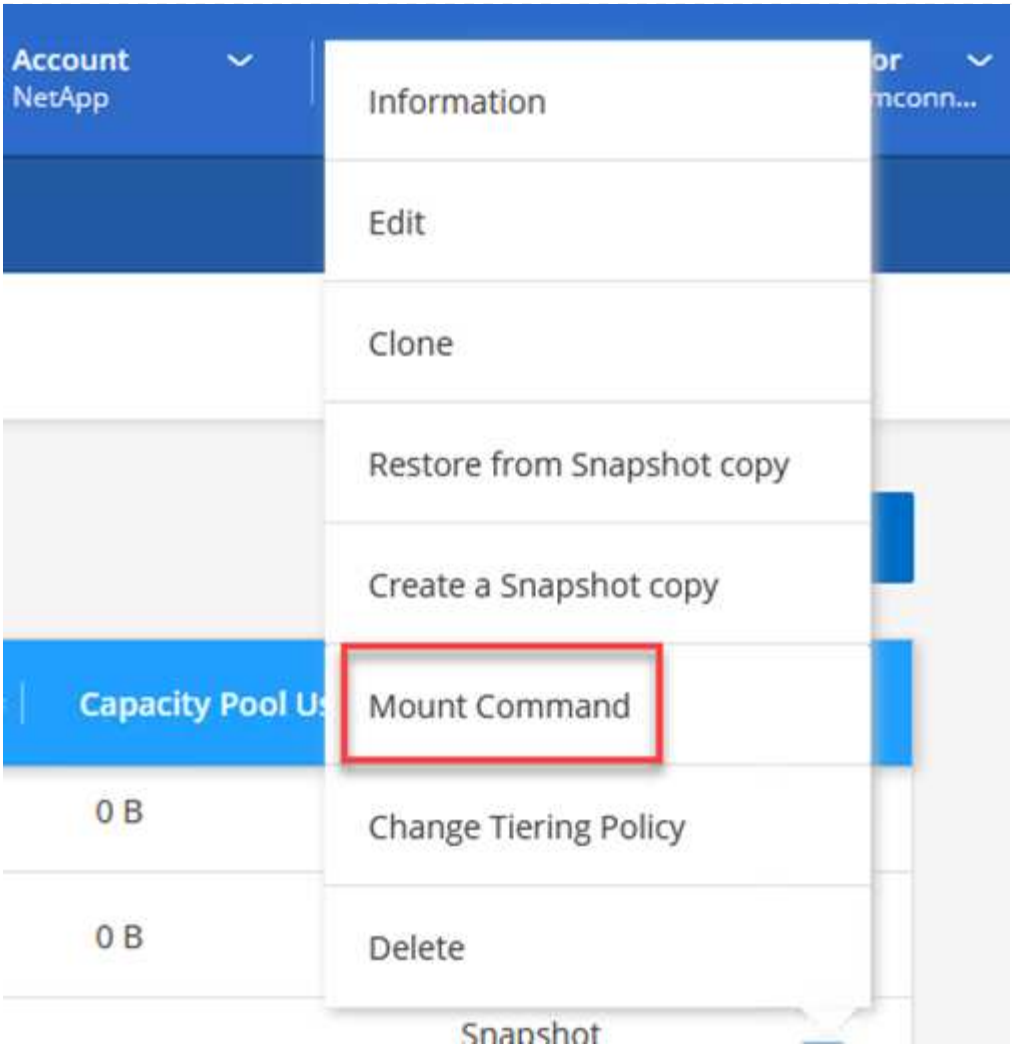
Oracle Serverに**NFS**ボリュームをマウントする

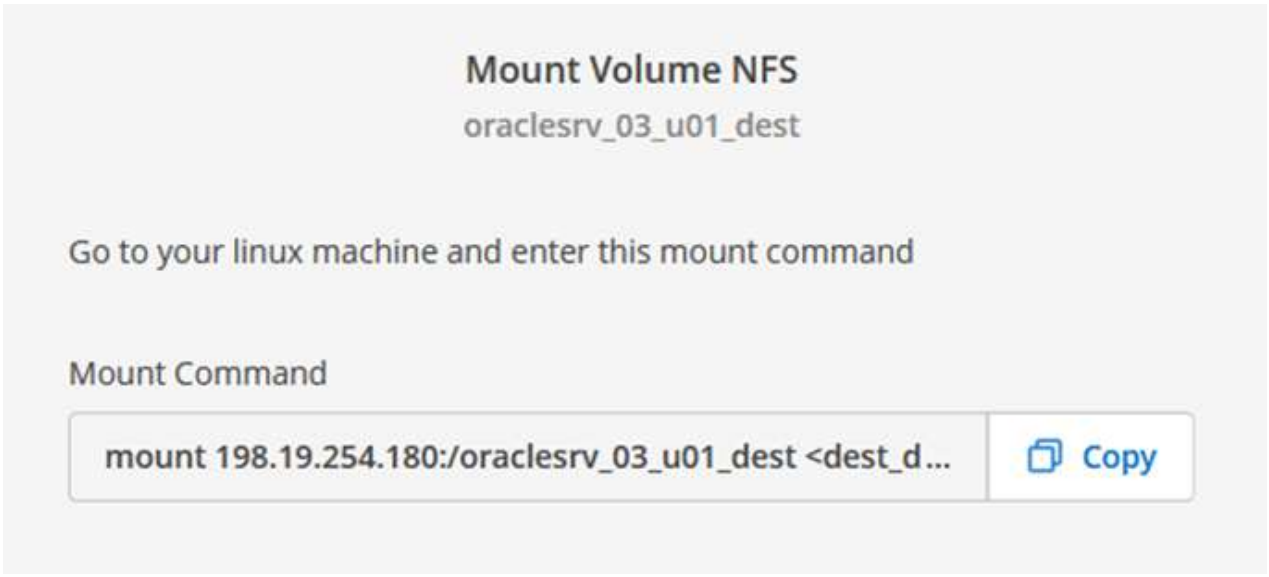
Cloud Manager では、Oracle データベース ファイルとログを含む NFS ボリュームをマウントするための正しい NFS LIF IP アドレスを指定したマウント コマンドを取得できます。

1. Cloud Manager で、FSx クラスターのボリュームのリストにアクセスします。



2. アクション メニューから [マウント コマンド] を選択し、Oracle Linux サーバーで使用するマウント コマンドを表示およびコピーします。





3. NFS ファイル システムを Oracle Linux Server にマウントします。 NFS 共有をマウントするためのディレクトリは、Oracle Linux ホストにすでに存在します。
4. Oracle Linux サーバーから、mount コマンドを使用して NFS ボリュームをマウントします。

```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

Oracle データベースに関連付けられているボリュームごとにこの手順を繰り返します。

再起動後もNFSマウントを永続化するには、 `/etc/fstab`マウント コマンドを含めるファイル。

5. Oracle サーバーを再起動します。 Oracle データベースは正常に起動し、使用可能になります。

フェイルバック

このソリューションで概説されているフェイルオーバー プロセスが正常に完了すると、 SnapCenterと Veeam は AWS で実行されているバックアップ機能を再開し、FSx ONTAPは元のオンプレミス データセンターとの既存のSnapMirror関係がないプライマリ ストレージとして指定されます。オンプレミスで通常の機能が再開されたら、このドキュメントで説明されているプロセスと同じプロセスを使用して、オンプレミスのONTAPストレージ システムにデータをミラーリングできます。

このドキュメントでも説明されているように、 SnapCenterを構成して、FSx ONTAPのアプリケーション データ ボリュームをオンプレミスのONTAPストレージ システムにミラーリングすることができます。同様に、スケールアウト バックアップ リポジトリを使用してバックアップ コピーを Amazon S3 に複製するように Veeam を構成して、それらのバックアップがオンプレミス データセンターにある Veeam バックアップ サーバーにアクセスできるようにすることができます。

フェイルバックはこのドキュメントの範囲外ですが、フェイルバックはここで概説した詳細なプロセスとほとんど変わりません。

まとめ

このドキュメントで紹介するユースケースは、 NetAppと VMware の統合を強調する実証済みの災害復旧テクノロジに重点を置いています。 NetApp ONTAPストレージ システムは、実績のあるデータ ミラーリング テクノロジを提供し、組織がオンプレミスと主要なクラウド プロバイダーが提供するONTAPテクノロジにまたがる災害復旧ソリューションを設計できるようにします。

FSx ONTAP on AWS は、 SnapCenterおよびSyncMirrorとのシームレスな統合を可能にし、アプリケーション データをクラウドに複製するソリューションの 1 つです。 Veeam Backup & Replication は、 NetApp ONTAP ストレージ システムと適切に統合され、vSphere ネイティブ ストレージへのフェイルオーバーを提供できる、もう 1 つのよく知られたテクノロジーです。

このソリューションは、SQL Server および Oracle アプリケーション データをホストするONTAPシステムのゲスト接続ストレージを使用した災害復旧ソリューションを提示しました。 SnapCenterとSnapMirrorは、ONTAPシステム上のアプリケーション ボリュームを保護し、クラウドにある FSx または CVO に複製するための、管理しやすいソリューションを提供します。 SnapCenter は、すべてのアプリケーション データを VMware Cloud on AWS にフェイルオーバーするための DR 対応ソリューションです。

著作権に関する情報

商標に関する情報